Arithmetic properties of j-function

A thesis submitted in partial fulfillment of the requirements for the award of the degree of

MASTER OF SCIENCE

by

JISHU DAS
13MS109

under

Dr. SWARNENDU DATTA

to the

DEPARTMENT OF MATHEMATICS AND STATISTICS

INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH KOLKATA
April, 2018

Declaration

I hereby declare that this thesis is my own work and to the best of my knowledge, it contains no materials previously published or written by any other person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at IISER Kolkata or any other educational institution, except where due acknowledgement is made in the thesis.

April, 2018	Jishu Das
IISER Kolkata	13MS109

Certification of the Supervisor

This is to certify that the thesis entitled "Arithmetic properties of j-function" is a bonafide work of Jishu Das and has been carried out under my supervision. This work has not been submitted for a degree or diploma at IISER Kolkata or any other educational institution. It contains no materials previously published or written by any other person, or substantial proportions of material which have been accepted for the award of any other degree or diploma elsewhere, except where due references are made in the thesis.

April, 2018
IISER Kolkata

Dr. Swarnendu Datta
Assistant Professor

Acknowledgement

I would first like to thank my MS thesis guide Dr. Swarnendu Datta, who helped me and guided me during the entire period of my thesis. He has been the most kindest person I have ever met in my life. Having worked two years under him was the best part of my life in pursuing mathematics. The things I have learned from him is ever going to educate and inspire me through out my life. It was an honor working under his supervision.

I would like to express my profound gratitude towards the faculties of IISER Kolkata. The whole IISER Kolkata fraternity and the environment helped me to learn a lot.

I am also indebted towards all the teachers I ever had in my life. Without the lessons taught by them, I would not have reached this stage.

My friends at IISER Kolkata were amazing and their presence in good and bad times was necessary. I would personally like to thank Bandhan Panda for his constant support and Sharon Robins for his discussions regarding the thesis.

Finally, I am grateful to my parents for supporting me through every ups and downs. They have always encouraged me to do good and try to be a better person.

Abstract

Modular forms play an significant role in number theory. They also appear in areas like algebraic topology and string theory. The j-function is a very special function in the theory of modular forms. In particular, modular forms of weight zero are polynomials in j-function which we prove in this thesis. The main goal of this thesis, however will be to explore some important properties of j-function, define modular functions for $\Gamma_0(m)$ and give a classification of it. Then we define the modular equation, explore some of its properties and use these properties to show that $j(O_K)$ is an algebraic integer where O_K is the ring of integers of $\mathbb{Q}(\sqrt{-n})$ for n being a square free natural number.

Contents

1 The j-function **3**

1.1 The Weirstrass $\wp$-function 3

1.2 Differential equation satisfied by $\wp$ 6

1.3 The j-function as an action of $SL_2(\mathbb{Z})$ 11

1.4 The q-expansion of j-function 15

2 Modular functions for $\Gamma_0(m)$ **20**

2.1 Classification of modular functions for $SL_2(\mathbb{Z})$ 22

2.2 Cosets of $C(m)$ in $\Gamma_0(m)$ 23

3 The Modular Equation **25**

3.1 Classification of modular functions for $\Gamma_0(m)$ 27

3.2 Arithmetic properties of $\Phi_m(X, Y)$ 28

3.3 Correspondence between roots of $\Phi_m(X, Y)$ and cyclic sublattices of index m 29

3.4 Ring of integers of $\mathbb{Q}(\sqrt{-n})$ 32

1 The j-function

Before defining the j-function for a given lattice we start with some basic definitions.

Definition 1.1. A lattice in $\mathbb{C}$ is a subgroup of the form $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ where $\{\omega_1,\omega_2\}$ form a $\mathbb{R}$ basis of $\mathbb{C}$ as a vector space over $\mathbb{R}$.

Whenever we mention lattice, we will refer to a lattice in $\mathbb{C}$. For example $\mathbb{Z}\oplus\mathbb{Z}i = \{m+ni \mid m,n \in \mathbb{Z}\}$ is one of the simple lattices one can consider. Now we define G_k of a lattice for $k \in \mathbb{N}$ and $k > 2$.

Lemma 1.1. *Let L be a lattice and let $G_k(L) = \sum_{\omega\in L\setminus\{0\}} \frac{1}{\omega^k}$. Then for $k > 2$ the series $G_k(L)$ absolutely converges.*

Proof. Let $\{\omega_1, \omega_2\}$ be a basis of L and let $L_n = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{N}$ and $-n \leq a, b \leq n\}$. We have $L_n \subset L_{n+1}$ for $n \in \mathbb{N} \cup \{0\}$ and

$$L = \bigsqcup_{n=1}^{\infty} L_n \setminus L_{n-1}$$

where $\bigsqcup$ stands for disjoint union.

We note that both a and b in D_n have $(2n+1)$ number of choices which implies that $|L_n| = (2n+1)^2$ and $|L_n \setminus L_{n-1}| = (2n+1)^2 - (2n-1)^2 = 8n$.

Let L_n^o denotes the set of complex numbers which are inside of the parallelogram formed by the points $\{-n\omega_1 - n\omega_2, -n\omega_1 + n\omega_2, n\omega_1 - n\omega_2, n\omega_1 + n\omega_2\}$. We denote the parallelogram by P. Now choose c such that $B(0, c) = \{z \in \mathbb{C} \mid |z| < c\} \subset L_1^o$. We claim that $B(0, nc) \subset L_n^o$ for $n \in \mathbb{N}$. If $z \in B(0, nc)$, then $|z| < nc$ equivalently $\frac{|z|}{n} < c$ which implies $\frac{z}{n} \in L_1^0$ and hence $z \in L_n^0$. If $\omega \in L_n \setminus L_{n-1}$, then $\omega \in P$ which implies $\omega \notin L_n^o$, so $|w| \geq nc$.

$$\begin{aligned} G_k(L) &= \sum_{\omega\in L\setminus\{0\}} \frac{1}{|\omega|^k} = \sum_{\omega\in L_n\setminus L_{n-1}, n\in\mathbb{N}} \frac{1}{|\omega|^k} \\ &\leq \sum_{n\in\mathbb{N}} 8n \cdot \frac{1}{(nc)^k} = \sum_{n\in\mathbb{N}} \frac{8}{c^k} \cdot \frac{1}{(n)^{k-1}} \end{aligned}$$

As $k > 2$, $k - 1 > 1$ and $\sum_{n\in\mathbb{N}} \frac{1}{(n)^{k-1}}$ converges absolutely. Therefore by comparison test, $G_k(L)$ is absolutely convergent.

□

1.1 The Weirstrass $\wp$-function

Definition 1.2. For a lattice L define

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right)$$

It is called the Weirstrass $\wp$-function. For a fixed lattice L we denote $\wp(z)$ instead of $\wp(z; L)$.

Definition 1.3. Let f be a meromorphic function on $\mathbb{C}$ and let L be a lattice in $\mathbb{C}$. f is a elliptic function with respect to L if $f(z+\omega) = f(z)$ for all $\omega \in L$.

Theorem 1.2. *(i) $\wp(z; L)$ is a meromorphic function on $\mathbb{C}$.*
(ii) $\wp(z; L)$ is elliptic with respect to L.
(iii) $\wp(z; L)$ has pole of order 2 for all $\omega \in L$ and is holomorphic for $\omega \in \mathbb{C} \setminus L$.

Proof. In order to prove (i) we use Weierstrass Theorem which states that limit of sequence of meromorphic functions converging on every compact subsets of the domain is meromorphic on the domain. We begin by estimating the term in the $\wp$-function.

$$\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} = \frac{\omega^2 - (z+\omega)^2}{\omega^2(z+\omega)^2} = \frac{-z(z+2\omega)}{\omega^2(z+\omega)^2}$$

If $|\omega| > 2|z|$, then

$$|z+\omega| \geq ||\omega| - |z|| \geq \frac{|\omega|}{2}$$

and

$$|z+\omega| \leq |z| + |\omega| < \frac{5|\omega|}{2}$$

.

Now

$$|\frac{z(z+2\omega)}{\omega^2(z+\omega)^2}| \leq \frac{|z||z+2\omega|}{|\omega|^2|\frac{\omega}{2}|^2}$$

$$\leq \frac{|z||\frac{5\omega}{2}|}{\frac{|\omega|^4}{4}} = 10\frac{|z|}{|\omega|^3}$$

If $z \notin L$, then

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L\setminus\{0\}, |\omega| \leq 2|z|} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) + \sum_{\omega \in L\setminus\{0\}, |\omega| > 2|z|} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

There is only finitely many number of terms except in

$$\sum_{\omega \in L\setminus\{0\}, |\omega| > 2|z|} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

but

$$\sum_{\omega \in L\setminus\{0\}, |\omega| > 2|z|} (\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}) \leq \sum_{\omega \in L\setminus\{0\}, |\omega| > 2|z|} 10\frac{|z|}{|\omega|^3}$$

As right hand side is convergent by Lemma 1.1, $\wp$ is convergent and well defined for $z \in \mathbb{C} \setminus L$.
Let $z_0 \in \mathbb{C}$ and consider an open ball B of radius r around it. Choose λ such

that $\lambda >\max_{z\in B}2|z|$. For $z \in B$, we have

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in L\setminus\{0\},|\omega|\leq\lambda}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) + \sum_{\omega\in L\setminus\{0\},|\omega|>\lambda}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

except in the last summation we have finite sum of meromorphic functions which is meromorphic.
On the other hand , if $|\omega| > \lambda$ then $|\omega| > 2|z|$, so

$$|\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}| \leq 10\frac{|z|}{|\omega|^3} \leq 5\frac{\lambda}{|\omega|^3}$$

and $\sum_{|\omega|>2\lambda} 5\frac{\lambda}{|\omega|^3}$ is convergent. Therefore by Weierstrass M-test the series $\sum_{\omega\in L\setminus\{0\},|\omega|>2|z|}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$ is uniformly convergent. This proves (i).

From the above uniform convergence we can write

$$\wp'(z) = \left(\frac{1}{z^2}\right)' + \sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)' = -2\left(\frac{1}{z^3} + \sum_{\omega\in L\setminus\{0\}}\frac{1}{(z+\omega)^3}\right)$$

$$= -2\left(\frac{1}{z^3} + \sum_{\omega\in L\setminus\{0\}}\frac{1}{(z+\omega)^3}\right) = -2\sum_{\omega\in L}\frac{1}{(z+\omega)^3}$$

Therefore $\wp'$ is elliptic. To show $\wp(z+\omega) = \wp(z)$ it is enough to show $\wp(z+\omega_1) = \wp(z)$ and $\wp(z+\omega_2) = \wp(z)$.
But $(\wp(z+\omega_1) - \wp(z))' = \wp'(z+\omega_1) - \wp(z) = 0$ since $\wp'(z+\omega_1) = \wp'(z)$. This implies $\wp(z+\omega_1) - \wp(z) = K$ where K is some constant. on putting $z = \frac{\omega_1}{2}$ we have $\wp(\frac{\omega_1}{2}) - \wp(\frac{-\omega_1}{2}) = K$ i.e. $K = 0$ since $\wp$ is an even function. Hence $\wp(z+\omega_1) = \wp(z)$. One can similarly show that $\wp(z+\omega_2) = \wp(z)$.

We see that $\wp(z)$ has a pole of order 2 at $z = 0 \in L$. Since $\wp(z)$ is periodic with respect to L, it has a pole of order 2 at points inside L. Also for $z \in \mathbb{C}\setminus L$, $\wp(z)$ is in fact holomorphic by above argument. ☐

Now we will see a connection between $\wp$ and G_k.

Lemma 1.3. *Let $\wp$ and G_k be defined as previously for a lattice L. Then in a neighbourhood of* 0 *we have,*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}$$

Proof. For $|x| < 1$ we have

$$\frac{1}{1-x} = \sum_{n=0}^{\infty}x^n$$

Since a power series can be differentiated terms by term within its radius of convergence, we have $\frac{1}{(1-x)^2} = 1 + \sum_{n=1}^{\infty}(n+1)x^n$. For $|z| < |\omega|$ we put $x = \frac{z}{\omega}$ in the previous series to get

$$\frac{1}{(1-\frac{z}{\omega})^2} = 1 + \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n$$

which implies

$$\frac{\omega^2}{(z-\omega)^2} - 1 = \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n$$

so that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}$$

Taking summation for $\omega \in L \setminus \{0\}$ we get

$$\sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right) = \sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) = \sum_{\omega\in L\setminus\{0\}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}$$

equivalently

$$\wp(z) - \frac{1}{z^2} = \sum_{n=1}^{\infty}\sum_{\omega\in L\setminus\{0\}}(n+1)\frac{z^n}{\omega^{n+2}}$$

(since the convergence is absolute)
Therefore

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}(L)z^n$$

$\wp(z)$ is an even function which implies all the coefficients of the odd powers are zero.
Therefore we have $\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}$. □

Definition 1.4. Let L be a lattice. We define $g_2(L) = 60G_4(L)$, $g_3(L) = 140G_6(L)$.

1.2 Differential equation satisfied by $\wp$

Lemma 1.4. *Let L be a lattice. The differential equation satisfied by $\wp(z)$ is given by*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

Proof. From Lemma 1.3, we have

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}$$

which implies

$$\wp'(z) = \frac{-2}{z^3} + \sum_{n=1}^{\infty} 2n(2n+1)G_{2n+2}(L)z^{2n-1}$$

. As $\wp'(z)$ has pole of order 3 and $\wp(z)$ has pole of order 2 at origin we compute first three terms of $\wp(z)^3$ and $\wp'(z)^2$. On doing so we find

$$\wp(z)^3 = \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6(L) + ...$$

and

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4(L)}{z^2} - 80G_6(L) + ...$$

where ... involves positive powers of z.
Now we consider

$$F(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4(L)\wp(z) + 140G_6(L)$$

and note that $F(0) = 0$. Since $G_4(L), G_6(L), \wp(z)$ and $\wp'(z)$ are periodic with respect to L, $F(z) = 0$ for all $z \in L$. $\wp$ and $\wp'$ are holomorphic on $\mathbb{C} \setminus L$, hence so is F. Thus F is entire. Image of $F(z)$ having $\mathbb{C}$ as domain is determined by considering $F(z)$ on $P = \{s\omega_1 + t\omega_2 \mid 0 \leq s, t \leq 1\}$ as $F(z)$ is periodic with respect to L. As P is compact and $F(z)$ is continuous, image of $F(z)$ having P as domain is also compact and hence bounded. By Liouville's Theorem $F(z)$ is constant which is identically 0.
Therefore

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

. □

Lemma 1.5. *Let L be a lattice, $\wp(z)$ be the Weierstrass ϕ function for L and let $\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(L)z^{2n}$ be its Laurent expansion. Then for $n \in \mathbb{N}$ the coefficient $(2n+1)G_{2n+2}(L)$ is a polynomial in $g_2(L)$ and $g_3(L)$ with rational coefficients independent of L.*

Proof. We start with

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$$

For simplicity we denote $(2n+1)G_{2n+2}(L)$ by a_n. In order to have a relation between the a_n's we differentiate the above equation, cancel $\wp'(z)$ and get $\wp''(z) = 6\wp(z)^2 - \frac{g_2(L)}{2}$.
We now put $\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} a_n z^{2n}$ in the above equation.
On one side we have

$$\wp''(z) = \frac{6}{z^4} + \sum_{n=1}^{\infty} 2n(2n-1)a_n z^{2n-2}$$

and on the other hand the coefficient of z^{2n-2} in $6\wp(z)^2 - \frac{g_2(L)}{2}$ is $6(2a_n + \sum_{i=1}^{n-2} a_i a_{n-1-i})$
So we have

$$2n(2n-1)a_n = 6\big(2a_n + \sum_{i=1}^{n-2} a_i a_{n-1-i}\big)$$

equivalently

$$(n(2n-1)-6)a_n = 3\sum_{i=1}^{n-2} a_i a_{n-1-i}$$

or

$$(2n^2-n-6)a_n = 3\sum_{i=1}^{n-2} a_i a_{n-1-i}$$

or

$$(2n+3)(n-2)a_n = 3\sum_{i=1}^{n-2} a_i a_{n-1-i}$$

Since $a_1 = 3G_4(L)$ and $a_2 = 5G_6(L)$ we have $g_2(L) = 60G_4(L) = 20a_1$, $g_3(L) = 140G_6(L) = 28a_2$ and $a_1 = \frac{g_2(L)}{20}$, $a_2 = \frac{g_3(L)}{28}$. By induction assume that a_j is a polynomial in $g_2(L)$ and $g_3(L)$ with rational coefficients for $1 \leq j \leq n$. From the recurrence relation we have

$$(2(n+1)+3)(n+1-2)a_{n+1} = 3\sum_{i=1}^{n+1-2} a_i a_{n+1-1-i}$$

i.e.

$$a_{n+1} = \frac{3\sum_{i=1}^{n-1} a_i a_{n-i}}{(2n+5)(n-1)}$$

Thus a_{n+1} is a polynomial in $g_2(L)$ and $g_3(L)$ with rational coefficients and proof is complete. ☐

Lemma 1.6. *Let $z, w \notin L$. If $\wp(z) = \wp(w)$ then $z \equiv \pm w$ mod L.*

Proof. Let $\{\omega_1, \omega_2\}$ be a basis of L. Let P denote the parallelogram $\{s\omega_1 + t\omega_2 \mid \delta \leq s, t \leq \delta + 1\}$ where $-1 < \delta < 0$ and Γ denote its boundary oriented in anticlockwise direction. Also every complex number is congruent to a number in P modulo L. Now let w be fixed. Consider $f(z) = \wp(z) - \wp(w)$. We can adjust δ in such a way that $f(z)$ has no zeroes or poles on Γ. By argument principle we have

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = Z - P$$

where Z denotes the number of zeroes and P denotes the number of poles of f counted with multiplicities. Since $\frac{f'(z)}{f(z)}$ is elliptic w.r.t L, the integrals on opposite sides on Γ cancels out implying $\int_\Gamma \frac{f'(z)}{f(z)}dz = 0$. This shows $Z = P$. As

$-1 < \delta < 0$, $f(z)$ has only one pole at 0 with multiplicity 2. So $f(z)$ has either two zeroes with multiplicity 1 or one zero with multiplicity 2.

Note that if $z \in \mathbb{C} \setminus L$, we can always have z' such that $z' \equiv z \bmod L$ and $z' \in P$. If $w \not\equiv -w \bmod L$ then $w, -w$ are equivalent to two different points say $w', -w'$ respectively inside P modulo L. However $f(w') = f(w) = \wp(w) - \wp(w) = 0$ and $f(-w') = f(-w) = \wp(-w) - \wp(w) = \wp(w) - \wp(w) = 0$ (as $\wp(z)$ is an even function. So in this case w and $-w$ are the roots of $f(z)$ meaning $\wp(z) = \wp(w)$ for $z = \pm w$. Also note that w has multiplicity 1 which implies $\wp'(w) \neq 0$.

Again if $w \equiv -w \bmod L$, then $2w \in L$. Since $\wp'(z)$ is elliptic w.r.t L and is an odd function we have $\wp'(w) = \wp'(w - 2w) = \wp'(-w) = -\wp(w)$ which implies $\wp'(w) = 0$, so that at w, $f(z)$ has multiplicity more than 1. As $f(z)$ has either two zeroes with multiplicity 1 or one zero with multiplicity 2, at w it has a zero with multiplicity 2. This completes the proof of the lemma. ☐

Lemma 1.7. *Let L be a lattice. Then the roots of the polynomial $4x^3 - g_2(L)x - g_3(L)$ are distinct.*

Proof. Let $w \notin L$. From the proof of the previous lemma we have that $\wp'(w) = 0$ if $2w \in L$. If $\wp'(w) = 0$, then $\wp'(-w) = 0$ as $\wp'$ is an odd function. Since $\wp'$ is elliptic and $\wp'(w) = \wp'(-w)$, we have $w \equiv -w \bmod L$ equivalently $2w \in L$. Also from the proof of the Lemma 1.4 we have $\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L)$. If $\{\omega_1, \omega_2\}$ is a basis of L then we have $\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2} \notin L$ and $\omega_1, \omega_2, \omega_1 + \omega_2 \in L$. So $\wp'(\frac{\omega_1}{2}) = \wp'(\frac{\omega_1}{2}) = \wp'(\frac{\omega_1+\omega_2}{2}) = 0$. The differential equation tells us that $\wp(\frac{\omega_1}{2}), \wp(\frac{\omega_2}{2}), \wp(\frac{\omega_1+\omega_2}{2})$ are roots of the equation $4x^3 - g_2(L)x - g_3(L)$ which are further distinct which follows from the lemma 1.6. ☐

Lemma 1.8. *Let L be a lattice. Then $\Delta(L) = g_2(L)^3 - 27g_3(L)^2 \neq 0$.*

Proof. Let e_1, e_2, e_3 be three roots of the polynomial, then

$$4x^3 - g_2(L)x - g_3(L) = 4(x - e_1)(x - e_2)(x - e_3)$$

On comparing coefficients of x^2, x and the constant term we have $e_1 + e_2 + e_3 = 0$, $e_1e_2 + e_2e_3 + e_3e_1 = \frac{-g_2(L)}{4}$ and $e_1e_2e_3 = \frac{g_3(L)}{4}$.
Note that $(e_1 - e_2)^2 = (e_1 + e_2)^2 - 4e_1e_2 = e_3^2 - 4e_1e_2$. So we have

$$(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 = (e_3^2 - 4e_1e_2)(e_2^2 - 4e_1e_3)(e_1^2 - 4e_2e_3)$$

$$= (e_1e_2e_3)^2 - 4((e_1e_2)^3 + (e_2e_3)^3 + (e_3e_1)^3) + 4^2(e_1e_2e_3)(e_1^3 + e_2^3 + e_3^3) - 4^3(e_1e_2e_3)^2$$

Now using the identity

$$(a + b + c)^3 = a^3 + b^3 + c^3 + 3(a + b)(b + c)(c + a)$$

where $a, b, c \in \mathbb{C}$ we have

$$\begin{gathered}
e_1^3 + e_2^3 + e_3^3 = (e_1 + e_2 + e_3)^3 - 3(e_1 + e_2)(e_2 + e_3)(e_3 + e_1) \\
= 0 + 3e_1e_2e_3 = 3e_1e_2e_3 \ \ as \ \ e_1 + e_2 + e_3 = 0 \\
and \ \ (e_1e_2)^3 + (e_2e_3)^3 + (e_3e_1)^3 \\
= (e_1e_2 + e_2e_3 + e_3e_1)^3 - 3(e_1e_2 + e_2e_3)(e_2e_3 + e_3e_1)(e_3e_2 + e_2e_1) \\
= (e_1e_2 + e_2e_3 + e_3e_1)^3 - 3e_1e_2e_3(-e_1)(-e_2)(-e_3) \\
= (e_1e_2 + e_2e_3 + e_3e_1)^3 + 3(e_1e_2e_3)^2
\end{gathered}$$

Now using $e_1e_2 + e_2e_3 + e_3e_1 = \frac{-g_2(L)}{4}$ and $e_1e_2e_3 = \frac{g_3(L)}{4}$
we get

$$(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 = \frac{g_2(L)^3 - 27g_3(L)^2}{16}$$

. Since e_1, e_2, e_3 are distinct $\Delta(L) \neq 0$ □

Definition 1.5. Let L be a lattice. Let $\Delta(L) = (g_2(L))^3 - 27(g_3(L))^2$. The j-function is defined to be

$$j(L) = 1728\frac{(g_2(L))^3}{(g_2(L))^3 - 27(g_3(L))^2} = 1728\frac{(g_2(L))^3}{\Delta(L)}$$

This makes sense as from Lemma 1.8 we have $\Delta(L) \neq 0$

Definition 1.6. Two lattices L and L' are said to be homothetic if there exists $\lambda \in \mathbb{C} \setminus \{0\}$ such that $L' = \lambda L$.

Theorem 1.9. *Let L and L' be lattices in $\mathbb{C}$. Then $j(L) = j(L')$ if and only if L and L' are homothetic.*

Proof. Let L and L' be homothetic, so that there is $\lambda \in \mathbb{C} \setminus \{0\}$ such that $L' = \lambda L$. Then

$$g_2(\lambda L) = 60G_4(\lambda L) = 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{(\lambda\omega)^4} = \lambda^{-4} \times 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4} = \lambda^{-4} g_2(L)$$

similarly $g_3(\lambda L) = \lambda^{-6} g_3(L)$ and

$$j(\lambda L) = 1728\frac{\lambda^{-12}(g_2(L))^3}{\lambda^{-12}(g_2(L))^3 - \lambda^{-12}(g_3(L))^2} = 1728\frac{(g_2(L))^3}{(g_2(L))^3 - 27(g_3(L))^2} = j(L)$$

.

Conversely, suppose L and L' are lattices such that $j(L) = j(L')$. Firstly we claim that there exists a non zero complex number λ such that $g_2(L') = \frac{g_2(L)}{\lambda^4}$ and $g_3(L') = \frac{g_3(L)}{\lambda^6}$.

When $g_2(L'), g_3(L') \neq 0$ we can choose λ such that $\lambda^4 = \frac{g_2(L)}{g_2(L')}$ and as $j(L') = j(L)$ we have

$$1728\frac{g_2(L')^3}{g_2(L')^3 - 27g_3(L')^2} = 1728\frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2}$$

equivalently

$$\frac{\lambda^{-12}g_2(L)^3}{\lambda^{-12}g_2(L)^3-27g_3(L')^2}=\frac{g_2(L)^3}{g_2(L)^3-27g_3(L)^2}$$

or

$$\lambda^{-12}g_2(L)^3-\lambda^{-12}27g_3(L)^2=\lambda^{-12}g_2(L)^3-27g_3(L')^2$$

Thus

$$\lambda^6=\pm\frac{g_3(L)}{g_3(L')}$$

If necessary replacing λ by $i\lambda$ we can assume that $\lambda^6=+\frac{g_3(L)}{g_3(L')}$ and we are done.

When $g_2(L')=0$, we must have $g_3(L')\neq 0$ since $\Delta(L')\neq 0$. we can choose λ such that $\lambda^6=\frac{g_3(L)}{g_3(L')}$. In such case $j(L')=j(L)$ implies $j(L)=0$, so that $g_2(L)=0$ and our claim holds.

When $g_3(L')=0$, we must have $g_2(L')\neq 0$ and $j(L')=1728=j(L)$ which implies $g_3(L)=0$. Then we can choose λ such that $\lambda^4(L)=\frac{g_2(L)}{g_2(L')}$ and this proves our claim completely.

Now we claim that $L'=\lambda L$. We have $g_2(L')=g_2(\lambda L)$ and $g_3(L')=g_3(\lambda L)$. Lemma 1.4 implies $\wp(z;L')$ and $\wp(z;L)$ have the same Laurent expansion expansion about origin, hence the two functions agree on a neighbourhood of origin and by analytic continuation we have $\wp(z;L')=\wp(z;L)$ everywhere in $\mathbb{C}\setminus L$. The set of poles for $\wp(z;L')$ is L' and the set of poles for $\wp(z;\lambda L)$ is λL which have to be equal i.e. $L'=\lambda L$. $\square$

Theorem 1.9 implies that upto homothety of lattices, j-function is an invariant which we say j-invariant of a lattice upto homothety. Apart from this notion of j-invariance there is another way to see j-invariant as a modular function over $SL_2(\mathbb{Z})$. In this notion, the j-function is a function on the upper half plane of the set of complex numbers, which we define below.

1.3 The j-function as an action of $SL_2(\mathbb{Z})$

Definition 1.7. Let $\mathfrak{h}$ denote the upper half plane i.e. $\mathfrak{h}=\{z\in\mathbb{C}\mid \operatorname{Im}(z)>0\}$. Let $\tau\in\mathfrak{h}$, $j(\tau)$ is defined as $j(\tau)=j(\mathbb{Z}\oplus\mathbb{Z}\tau)$.

We similarly define

$$g_2(\tau)=g_2(\mathbb{Z}\oplus\mathbb{Z}\tau)=60\sum_{m,n}{}'\frac{1}{(m+n\tau)^4}$$

and

$$g_3(\tau)=g_3(\mathbb{Z}\oplus\mathbb{Z}\tau)=140\sum_{m,n}{}'\frac{1}{(m+n\tau)^6}$$

where $\sum'_{m,n}$ denotes summation over all pairs of integer except the pair $(0,0)$. Therefore by Definition 1.5, $j(\tau)=1728\frac{g_2(\tau)^3}{\Delta(\tau)}$.

Now we consider the action of the group

$$SL_2(\mathbb{Z}) = \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{Z} \quad and \quad ad - bc = 1\}$$

on $\mathfrak{h}$ defined as follow : if $\tau \in \mathfrak{h}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, then $\gamma\tau = \frac{a\tau+b}{c\tau+d}$. We show that it is indeed an group action.

Lemma 1.10. *Let $G = SL_2(\mathbb{Z})$, $X = \mathfrak{h}$ and for $\tau \in \mathfrak{h}$, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ set $\gamma\tau = \frac{a\tau+b}{c\tau+d}$. Then G acts on X (on the left).*

Proof. We start with showing $\gamma\tau \in SL_2(\mathbb{Z})$. We have

$$\gamma\tau = \frac{a\tau + b}{c\tau + d} = \frac{(a\tau + b)(c\overline{\tau} + d)}{|c\tau + d|^2} = \frac{ac|\tau|^2 + bd + ad\tau + bc\overline{\tau}}{|c\tau + d|^2}$$

since $|\tau|^2, |c\tau + d|^2 \in \mathbb{R}$ and $\operatorname{Im}(\tau) = -\operatorname{Im}(\overline{\tau})$ we can write

$$Im(\gamma\tau) = \frac{ad - bc}{|c\tau + d|^2} Im(\tau) = \frac{Im(\tau)}{|c\tau + d|^2}$$

which is positive as $\operatorname{Im}(\tau) > 0$. This shows $\gamma\tau \in \mathfrak{h}$.
Clearly $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tau = \tau$.
If $\gamma_1 = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ and $\gamma_2 = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$, then $\gamma_1\gamma_2 = \begin{bmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{bmatrix}$

$$\gamma_1(\gamma_2\tau) = \gamma_1\left(\frac{a_2\tau + b_2}{c_2\tau + d_2}\right) = \frac{a_1\left(\frac{a_2\tau+b_2}{c_2\tau+d_2}\right) + b_1}{c_1\left(\frac{a_2\tau+b_2}{c_2\tau+d_2}\right) + d_1} = \frac{\left(\frac{a_1a_2\tau+a_1b_2+b_1c_2\tau+b_1d_2}{c_2\tau+d_2}\right)}{\left(\frac{c_1a_2\tau+c_1b_2+d_1c_2\tau+d_1d_2}{c_2\tau+d_2}\right)}$$

$$= \frac{(a_1a_2 + b_1c_2)\tau + (a_1b_2 + b_1d_2)}{(c_1a_2 + d_1c_2)\tau + (c_1b_2 + d_1d_2)} = (\gamma_1\gamma_2)\tau$$

Thus $SL_2(\mathbb{Z})$ acts on $\mathfrak{h}$. □

Definition 1.8. Let $\tau, \tau' \in \mathfrak{h}$. τ and τ' are $SL_2(\mathbb{Z})$ equivalent if there exists $\gamma \in SL_2(\mathbb{Z})$ such that $\tau' = \gamma\tau$.

Lemma 1.11. *Every point $\tau \in \mathfrak{h}$ is $SL_2(\mathbb{Z})$ equivalent to a point $\tau' \in \mathfrak{h}$ satisfying $|Re(\tau')| \leq \frac{1}{2}$ and $Im(\tau') \geq \frac{1}{2}$.*

Proof. If $\operatorname{Im}(\tau) \geq \frac{1}{2}$ then there is $m \in \mathbb{Z}$ such that $\tau' = \tau + m = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \tau$ satisfying —Re$(\tau')| \leq \frac{1}{2}$. We are done for the case when $\operatorname{Im}(\tau) \geq \frac{1}{2}$ as $\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$.

If $\mathrm{Im}(\tau) < \frac{1}{2}$, then from the argument just before we can assume there is τ' equivalent to τ satisfying $|\mathrm{Re}(\tau')| \leq \frac{1}{2}$. So we have $|\tau'| < \frac{1}{\sqrt{2}}$. Now

$$Im\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \tau' \right) = \frac{Im(\tau')}{|\tau'|^2} > 2\ Im(\tau')$$

Since $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in SL_2(\mathbb{Z})$, τ' is $SL_2(\mathbb{Z})$ equivalent to $\frac{-1}{\tau'}$. However by the above argument, we can choose τ'' equivalent τ' with imaginary part of τ'' more than twice of imaginary part of τ'. Proceeding finitely many times, we arrive at $\tilde{\tau}$ which is $SL_2(\mathbb{Z})$ equivalent τ' satisfying $\mathrm{Im}(\tilde{\tau}) \geq \frac{1}{2}$. So we have $\tilde{\tau}$ which is $SL_2(\mathbb{Z})$ equivalent to τ having the desired property. ☐

Lemma 1.12.

$$\lim_{Im(\tau)\to\infty} j(\tau) = \infty$$

Proof. Firstly we try to show $g_2(\tau)$ converges uniformly on every compact subsets of $\mathfrak{h}$. We have already showed that $g_2(\tau)$ is absolutely convergent. Note that $\mathbb{Z} \oplus \mathbb{Z}(\tau+1) = \mathbb{Z} \oplus \mathbb{Z}\tau$ which implies $g_2(\tau+1) = g_2(\tau)$. Thus by Lemma 1.11 it suffices to show the convergence is uniform where τ satisfies $|\mathrm{Re}(\tau)| \leq \frac{1}{2}$ and $\mathrm{Im}(z) \geq \epsilon$ with $0 < \epsilon < 1$. We claim that $|m + n\tau| \geq \frac{\epsilon}{2}\sqrt{m^2+n^2}$.
Once we show this we will have

$$|g_2(\tau)| \leq 60 \sum_{m,n}{}' \frac{1}{|m+n\tau|^4} \leq 60 \sum_{m,n}{}' \frac{16}{\epsilon^4 (m^2+n^2)^2}$$

By Weierstrass M-Test, uniform convergence will be shown once we see that the right part converges. Hence

$$\sum_{m,n}{}' \frac{1}{(m^2+n^2)^2} = \sum_{m,n}{}' \frac{1}{(|m+ni|^2)^2} = \sum_{\omega \in L\setminus\{0\}} \frac{1}{|\omega|^4}$$

(where $L = \{m + ni \mid m, n \in \mathbb{Z}\}$) is convergent by Lemma 1.1.
We now show that $|m + n\tau| \geq \frac{\epsilon}{2}\sqrt{m^2+n^2}$, which is equivalent to show

$$(m+an)^2 + b^2n^2 \geq \frac{\epsilon^2}{4}(m^2+n^2)$$

where $\tau = a + bi$ $(a, b \in \mathbb{R})$ whenever $|a| \leq \frac{1}{2}$ and $b \geq \epsilon$ with $\epsilon < 1$.
If $|m + an| \geq \frac{\epsilon}{2}|m|$, then

$$(m+an)^2 \geq \frac{m^2\epsilon^2}{4} \ \ and \ \ (nb)^2 \geq (n\epsilon)^2 > \frac{n^2\epsilon^2}{4}$$

which immediately implies the claim.
If $|m + an| \geq \frac{\epsilon}{2}|m|$, then $|m| < |n|$. Suppose not, then $|m| \geq |n|$ equivalently $-|an| \geq \frac{-|m|}{2}$ (as $|a| \leq \frac{1}{2}$). Hence

$$\frac{|m|}{2} \leq ||m| - |an|| \leq |m+an| < \frac{\epsilon|m|}{2} < \frac{|m|}{2}$$

which is a contradiction.
Again

$$(m+an)^2+(bn)^2 = m^2+a^2n^2+2man+b^2n^2 \geq m^2+a^2n^2-|m||n|+b^2n^2$$

$$> m^2+a^2n^2-|m|^2+b^2n^2 \geq \frac{m^2}{4}+\frac{n^2\epsilon^2}{4} \geq \frac{m^2\epsilon^2}{4}+\frac{n^2\epsilon^2}{4} = \frac{\epsilon^2}{4}(m^2+n^2)$$

One may similarly show the uniform convergences of $g_3(\tau)$ for every compact subsets of $\mathfrak{h}$.
We then compute limits of $g_2(\tau)$ and $g_3(\tau)$ as $\mathrm{Im}(\tau) \to \infty$.

$$\lim_{Im(\tau)\to\infty} g_2(\tau) = \lim_{Im(\tau)\to\infty} 60 \sum_{m,n}{}' \frac{1}{(m+n\tau)^4}$$

$$= \lim_{Im(\tau)\to\infty} 60\Bigg(2\sum_{m=1}^{\infty}\frac{1}{m^4} + \sum_{m,n=-\infty, n\neq 0}^{\infty}\frac{1}{(m+n\tau)^4}\Bigg)$$

on using the uniform convergence shown above and taking the limit inside the summation we have

$$\lim_{Im(\tau)\to\infty} g_2(\tau) = 120\sum_{m=1}^{\infty}\frac{1}{m^4} = 120\frac{\pi^4}{90} = \frac{4}{3}\pi^4$$

A proof of $\sum_{m=1}^{\infty}\frac{1}{m^4} = \frac{\pi^4}{90}$ can be found at reference. Similarly using $\sum_{m=1}^{\infty}\frac{1}{m^6} = \frac{\pi^4}{945}$ from reference we can show

$$\lim_{Im(\tau)\to\infty} g_3(\tau) = \frac{8}{27}\pi^6$$

consequently these limits imply

$$\lim_{Im(\tau)\to\infty} \Delta(\tau) = (\frac{4}{3}\pi^4)^3 - 27(\frac{8}{27}\pi^6)^2 = 0$$

. Thus we conclude

$$\lim_{Im(\tau)\to\infty} j(\tau) = \infty$$

□

Theorem 1.13. *(i) $j(\tau)$ is a holomorphic function on $\mathfrak{h}$.*
(ii) Let $\tau, \tau' \in \mathfrak{h}$. $j(\tau) = j(\tau')$ if τ', τ are $SL_2(\mathbb{Z})$ equivalent.
(iii) $j : \mathfrak{h} \longrightarrow \mathbb{C}$ is surjective.

Proof. By lemma 1.8 which states $\Delta(L) \neq 0$ for a lattice L, it is enough to show that $g_2(\tau)$ and $g_3(\tau)$ are holomorphic on $\mathfrak{h}$. However from the proof of lemma 1.12 we have $g_2(\tau), g_3(\tau)$ converging uniformly on every compact subset of $\mathfrak{h}$. Hence both $g_2(\tau)$ and $g_3(\tau)$ are holomorphic which imply $\Delta(\tau)$ and $j(\tau)$ are holomorphic on $\mathfrak{h}$. This proves (i).

Let $\tau, \tau' \in \mathfrak{h}$ such that $\tau' = \gamma\tau$ for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. By definition 1.7, we see that $g_2(\tau') = \frac{g_2(\tau)}{(c\tau+d)^4}$ and $g_3(\tau') = \frac{g_3(\tau)}{(c\tau+d)^6}$. Using these two identities we see that

$$j(\tau') = 1728\frac{g_2(\tau')^3}{g_2(\tau')^3 - 27g_3(\tau')^2} = 1728\frac{(c\tau+d)^{12}g_2(\tau)^3}{(c\tau+d)^{12}(g_2(\tau)^3 - 27g_3(\tau)^2)} = j(\tau)$$

Hence proof of (ii) is done.

Image of j-function is an open subset of $\mathbb{C}$ by open mapping theorem. To show that j is surjective it is now sufficient if we show that image is closed. Let $j(\tau_n)$ be a sequence converging to $w \in \mathbb{C}$. By Lemma 1.11 we can assume that for $n \in \mathbb{N}, \tau_n \in \{\tau \in \mathfrak{h} \mid |\operatorname{Re}(\tau)| \leq \frac{1}{2}, |\operatorname{Im}(\tau)| \geq \frac{1}{2}\}$. We claim that imaginary parts of $j(\tau_n)'s$ is bounded. Suppose not, then by Lemma 1.12 there will be a subsequence $j(\tau_{n_k})$ diverging to ∞ which is impossible as $j(\tau_n)$ is convergent. Hence $\tau_n's$ lie in a compact subset of $\mathfrak{h}$, so there is a subsequence τ_{n_k} converging to $\tau \in \mathfrak{h}$. Therefore

$$w = \lim_{n\to\infty} j(\tau_n) = \lim_{k\to\infty} j(\tau_{n_k}) = j(\lim_{k\to\infty} \tau_{n_k}) = j(\tau)$$

as j is continuous on $\mathfrak{h}$. Therefore j is surjective. □

1.4 The q-expansion of j-function

Lemma 1.14. *Let $z \in \mathbb{C} \setminus \mathbb{Z}$. Then we have*

$$\pi\cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty}\left(\frac{1}{z-n} + \frac{1}{z+n}\right)$$

Proof. Let $z \in \mathbb{C} \setminus \mathbb{Z}$, then $\cot(\pi z)$ is holomorphic on $\mathbb{C} \setminus \mathbb{Z}$, so we focus on the infinite sum. Firstly we see that it is absolutely convergent. The sum $\sum_{n\in\mathbb{N}} |\frac{z^2}{z^2-n^2}|$ is convergent by comparison test and the fact that $\sum_{n\in N}\frac{1}{n^2}$ converges. Let D be a neighbourhood around z whose closure in $\mathbb{C}$ does not intersect $\mathbb{C} \setminus \mathbb{Z}$. Hence for all $w \in D$, $|w| \leq \epsilon$ for some $\epsilon > 0$ and $\epsilon \notin \mathbb{N}$. We will show

$$f(z) = \frac{1}{z} + \sum_{n=1}^{\infty}\left(\frac{1}{z-n} + \frac{1}{z+n}\right)$$

is holomorphic on D, so in particular is holomorphic at z. For $w \in D$, $|\frac{w^2}{w^2-n^2}| \leq \frac{\epsilon^2}{\epsilon^2-n^2}$ as $|w^2 - n^2| \geq ||w|^2 - n^2| \geq |\epsilon^2 - n^2|$ and since $\sum_{n=1}^{\infty}\frac{\epsilon^2}{\epsilon^2-n^2}$ is convergent, f is uniformly convergent on D. By applying Weirstrass theorem we see that f is holomorphic on D.

f is periodic with period 1 as the difference of the partial sum converges to zero. One also checks that both $\pi\cot(\pi z)$ and $f(z)$ have a simple pole for every integer. Thus it follows that $g(z) = \pi\cot(\pi z) - f(z)$ is an entire function with

period 1. Once we show g is bounded everywhere, we will have $g(z) = k$ for some constant $k \in \mathbb{C}$. Furthermore g is odd would imply $k = 0$.
Since both f and $\pi \cot(\pi z)$ are odd functions g is odd and Im (g) is determined by its image on $\mathfrak{h} \cup \mathbb{R}$. To show g is bounded it is sufficient if we show that f remains bounded as $\mathrm{Im}(z) \to \infty$ since by the formula

$$\pi \cot(\pi z) = \pi i \frac{e^{2\pi i z} + 1}{e^{2\pi i z} - 1}$$

we have $\pi \cot(\pi z)$ tends to $-\pi i$ as $\mathrm{Im}(z) \to \infty$. Suppose that $z = it$, then $f(z) = \frac{1}{it} - 2i \sum_{n \in \mathbb{N}} \frac{t}{t^2+n^2}$. As $\frac{t}{t^2+n^2} \leq \int_{n-1}^{t} \frac{t}{t^2+x^2} dx$ and the integrand has $\tan^{-1} \frac{x}{t}$, the series is bounded by

$$\int_0^\infty \frac{t}{t^2+x^2} dx = \left[\tan^{-1} \frac{x}{t} \right]_0^\infty = \frac{\pi}{2}$$

Since f has period 1, we can assume $z = it + r$, where $|r| \leq \frac{1}{2}$. Note that t can be chosen large enough such that $\frac{1}{2}(t^2 + n^2) \geq \frac{1}{4} + t$ for $n \in \mathbb{N}$ and $t \geq \frac{1}{2}$ as we wish to show f is bounded for $t \to \infty$. Now

$$|z^2 - n^2| = |-(t^2+n^2) + r^2 + 2itr| \geq |(t^2 + n^2 - r^2) - (2tr)|$$

$$\geq |t^2 + n^2 - \frac{1}{4} - t| \geq \frac{1}{2}(t^2 + n^2)$$

and $|z| = |it + r| \leq t + \frac{1}{2} \leq 2t$ imply

$$\sum_{n \in \mathbb{N}} \left(\frac{1}{z-n} + \frac{1}{z+n} \right) = \sum_{n \in \mathbb{N}} \left| \frac{2z}{z^2 - n^2} \right| \leq 2 \sum_{n \in \mathbb{N}} \frac{t}{t^2+n^2} \leq \pi$$

and the proof of the lemma is complete. ☐

Lemma 1.15. *Let $\tau \in \mathfrak{h}$ and $n \in \mathbb{N}$. We have the following*

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3} \sum_{r=1}^{\infty} r^3 e^{2\pi i r n \tau}$$

and

$$\sum_{m=-\infty}^{+\infty} \frac{1}{(m+n\tau)^6} = \frac{-8\pi^6}{15} \sum_{r=1}^{\infty} r^5 e^{2\pi i r n \tau}$$

Proof. We begin with the partial fraction decomposition of cotangent which we proved in the previous lemma.

$$\pi \; cot \; \pi\tau = \frac{1}{\tau} + \sum_{m=-\infty, m\neq 0}^{\infty} \left(\frac{1}{\tau+m} - \frac{1}{m} \right)$$

. As $\tau = x + iy \in \mathfrak{h}$ with $x \in \mathbb{R}$ and $y > 0$,

$$|e^{2\pi i\tau}| = |e^{2\pi ix-2\pi y}| = |e^{2\pi ix}||e^{-2\pi y}| < 1$$

as $|e^{2\pi ix}| = 1$ and $|e^{-2\pi y}| < 1$
Denote $q = e^{2\pi i\tau}$, then we have $|q| < 1$ and we see that

$$\pi\ \cot\ \pi\tau = \pi\frac{\cos\ \pi\tau}{\sin\ \pi\tau} = \pi\frac{(\ \cos\ \pi\tau + i\ \sin\ \pi\tau)\ \cos\ \pi\tau}{(\ \cos\ \pi\tau + i\ sin\ \pi\tau)\ \sin\ \pi\tau} = \pi\frac{(\frac{1+\ \cos\ 2\pi\tau}{2}) + i(\frac{\sin\ 2\pi\tau}{2})}{(\frac{\sin\ 2\pi\tau}{2}) + i(\frac{1-\ \cos\ 2\pi\tau}{2})}$$

$$= \pi i\frac{1 + (\ \cos\ 2\pi\tau + i\ \sin\ 2\pi\tau)}{(\ \cos\ 2\pi\tau + i\ \sin\ 2\pi\tau) - 1} = \pi i\frac{q+1}{q-1} = -\pi i\left(\frac{q}{1-q} + \frac{1}{1-q}\right)$$

$$= -\pi i\left(\sum_{r=0}^{\infty} q^r + \sum_{r=1}^{\infty} q^r\right) = \pi i\left(1 + 2\sum_{r=1}^{\infty} q^r\right)$$

If we replace $q = e^{2\pi i\tau}$ and use this identity in partial decomposition of cotangent we will have

$$\frac{1}{\tau} + \sum_{m=-\infty,m\neq 0}^{\infty}\left(\frac{1}{\tau+m} - \frac{1}{m}\right) = -\pi i\left(1 + 2\sum_{r=1}^{\infty} e^{2\pi ir}\right)$$

Differentiating three times we have

$$\frac{-3!}{\tau^2} - \sum_{m=-\infty,m\neq 0}^{\infty} \frac{3!}{(\tau+m)^4} = -(2\pi i)^4\sum_{r=1}^{\infty} r^3 e^{2\pi ir\tau}$$

equivalently

$$\sum_{m=-\infty}^{\infty} \frac{1}{(\tau+m)^4} = \frac{8\pi^4}{3}\sum_{r=1}^{\infty} r^3 e^{2\pi ir\tau}$$

on replacing τ by $n\tau$ we have

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^4} = \frac{8\pi^4}{3}\sum_{r=1}^{\infty} r^3 e^{2\pi irn\tau}$$

Similarly differentiating five time and the replacing τ by $n\tau$ we have

$$\sum_{m=-\infty}^{\infty} \frac{1}{(m+n\tau)^6} = \frac{-8\pi^6}{15}\sum_{r=1}^{\infty} r^5 e^{2\pi irn\tau}$$

□

Lemma 1.16. *If $\tau \in \mathfrak{h}$, then we have*

$$g_2(\tau) = \frac{4\pi^4}{3}\left(1 + 240\sum_{k=1}^{\infty} \sigma_3(k)e^{2\pi ik\tau}\right)$$

and

$$g_3(\tau) = \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty}\sigma_5(k)e^{2\pi ik\tau}\right)$$

where $\sigma_t(k) = \sum_{d|k} d^t$ *for* $t \in \mathbb{N}$.

Proof. We shall prove the first one and the second one will follow similarly. We have

$$g_2(\tau) = 60 \sum_{m,n=-\infty,(m,n)\neq(0,0)}^{+\infty} \frac{1}{(m+n\tau)^4}$$

$$= 60 \left[\sum_{m=-\infty,m\neq 0,n=0}^{\infty} \frac{1}{m^4} + \sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\left(\frac{1}{(m+n\tau)^4} + \frac{1}{(m-n\tau)^4}\right)\right]$$

$$= 60 \left[\frac{2\pi^4}{90} + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty}\frac{1}{(m+n\tau)^4}\right]$$

$$= 60\left[\frac{2\pi^4}{90} + \frac{16\pi^4}{3}\sum_{n=1}^{\infty}\sum_{r=1}^{\infty} r^3 q^{nr}\right]$$

where $q = e^{2\pi i\tau}$. As n, r varies over natural numbers nr also vary over natural numbers, so we collect the coefficients for which nr is constant in the double sum and note that for a fixed $nr = k$ (say) we get precisely those r^3 terms as coefficient of q^{nr} for which r divides k as r divides nr. Therefore we have

$$g_2(\tau) = \frac{4\pi^4}{3}\left[1 + 240\sum_{k=1}^{\infty}\left(\sum_{r|k} r^3\right)q^k\right]$$

$$g_2(\tau) = \frac{4\pi^4}{3}\left[1 + 240\sum_{k=1}^{\infty}\sigma_3(k)e^{2\pi ik\tau}\right]$$

. ☐

Theorem 1.17. *Let* $\tau \in \mathfrak{h}$. *We have*

$$\Delta(\tau) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}$$

where the $\tau(n)$ *are integers with* $\tau(1) = 1$ *and* $\tau(2) = -24$.

The arithmetical function $\tau(n)$ is called Ramanujan's tau function.

Proof. For simplicity we denote

$$q = e^{2\pi i\tau}, \ \ A = \sum_{n=1}^{\infty}\sigma_3(n)q^n \ \ \textit{and} \ \ B = \sum_{n=1}^{\infty}\sigma_5(n)q^n$$

. We will use the previous lemma. We have

$$\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$$

$$= \frac{64\pi^{12}}{27}\left[(1+240A)^3 - (1-504B)^2\right]$$

Note that A and B have integer coefficients.

$$\begin{gathered}(1+240A)^3 - (1-504B)^2 \\ = 1 + 720A + 3(240)^2A^2 + (240)^3A^3 - 1 + 1008B - (504)^2B^2 \\ = 12^2(5A+7B) + 12^3(100A^2 - 147B^2 + 8000A^3)\end{gathered}$$

But $5A + 7B = \sum_{n=1}^{\infty}[5\sigma_3(n) + 7\sigma_5(n)]q^n$.
Observe that

$$5d^3 + 7d^5 = d^3(5+7d^2) \equiv d^3(d^2-1) = d^2[(d-1)(d)(d+1)]\ (mod\ \ 3)$$

since product of three consecutive integers is divisible by 3,
$d^3(5+7d^2) \equiv 0 \pmod 3$.

Again $d^3(5+7d^2) \equiv d^3(1-d^2) \pmod 4$. If d is even, then d^3 is divisible by 4 and if d is odd, then $d-1$ and $d+1$ are even implying their product will be divisible by 4. So we have $d^3(5+7d^2) \equiv 0 \pmod 4$.

Thus we have $d^3(5+7d^2) \equiv 0 \pmod{12}$. This shows 12 is a factor of the power series $5A+7B$ and 12^3 is a factor of $(1+240A)^3 - (1-504B)^2$.
Therefore we have

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left(12^3\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}\right) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)e^{2\pi in\tau}$$

where $\tau(n)$ are integers as in the power series expansion of
$\left[\frac{(5A+7B)}{12} + (100A^2 - 147B^2 + 8000A^3)\right]$ coefficients are integers.
Now we look for the coefficient of x in $\left[\frac{(5A+7B)}{12} + (100A^2 - 147B^2 + 8000A^3)\right]$
which is $\frac{5\sigma_3(1)+7\sigma_5(1)}{12} = 1$. so $\tau(1) = 1$.

Similarly for $\tau(2)$, we look for coefficient of x^2 in
$\left[\frac{(5A+7B)}{12} + (100A^2 - 147B^2 + 8000A^3)\right]$ which is

$$\left[\frac{5\sigma_3(2) + 7\sigma_5(2)}{12} + 100\sigma_3(1) - 147\sigma_5(1)\right] = \left[\frac{5\times 9 + 7\times 33}{12} - 47\right] = 23 - 47 = -24$$

so $\tau(2) = -24$. □

Theorem 1.18. *If $\tau \in \mathfrak{h}$, then we have*

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n$$

where $q = e^{2\pi i \tau}$ and $c(n)$ are integers.

Proof. In order to avoid tedious calculation we denote any power series in q with power of q starting from two or more than two and integer coefficients as I. If $q = e^{2\pi i \tau}$, then we have

$$g_2^3(\tau) = \frac{64\pi^{12}}{27}(1 + 240q + I)^3 = \frac{64\pi^{12}}{27}(1 + 720q + I)$$

and

$$\Delta(\tau) = \frac{64\pi^{12}}{27}\left[12^3 q(1 - 240q + I)\right]$$

hence

$$j(\tau) = 1728\frac{g_2^3(\tau)}{\Delta(\tau)} = \frac{1 + 720q + I}{q(1 - 24q + I)}$$

$$= \frac{(1 + 720q + I)(1 + I)}{q(1 - 24q + I)} = \frac{(1 + 720q + I)(1 + 24q + I)}{q} = \frac{1 + 744q + I}{q}$$

as $(1 + 24q + I)(1 - 24q + I) = (1 + I)$
Therefore

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n$$

where $c(n)$ are integers as I has integer coefficients. ☐

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n=1}^{\infty} c(n) q^n$$

is called the q-expansion of j- function. In the next section we learn more about the q-expansion of a modular function.

2 Modular functions for $\Gamma_0(m)$

Now we will focus on a particular subgroup $\Gamma_0(m)$ of $SL_2(\mathbb{Z})$ where m being a positive integer, which will enable us to define modular functions, which is defined as

$$\Gamma_0(m) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \;\mid\; c \equiv 0 \pmod{m} \right\}$$

.

Definition 2.1. f is a modular function for $\Gamma_0(m)$ if f is defined on $\mathfrak{h}$ satisfying
(i)f is meromorphic on $\mathfrak{h}$,
(ii) $f(\gamma\tau) = f(\tau)$ for $\gamma \in \Gamma_0(m)$,
(iii) The q-expansion of $f(\gamma\tau)$ has only finitely many non zero coefficients for negative powers for all $\gamma \in SL_2(\mathbb{Z})$.

In order to understand (iii) we need to consider the following paragraph. Let f is a function defined on $\mathfrak{h}$ satisfying (i) and (ii), we claim that $f(\gamma\tau)$ has period m for $\gamma \in SL_2(\mathbb{Z})$. Proof of this is as follows.

Proof. If $U = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ and $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, then

$$\gamma U \gamma^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \begin{bmatrix} d & -b \\ -c & d \end{bmatrix} = \begin{bmatrix} a & am+b \\ c & cm+d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & d \end{bmatrix}$$

$$= \begin{bmatrix} ad-bc-acm & -ab+adm+bd \\ dc-c^2m-dc & -bc+dcm+d^2 \end{bmatrix} = \begin{bmatrix} 1-acm & adm+bd-ab \\ -c^2m & cdm+d^2-bc \end{bmatrix} \in \Gamma_0(m)$$

Now $f(\gamma(\tau+m)) = f(\gamma U\tau) = f(\gamma U(\gamma^{-1}\gamma)\tau) = f((\gamma U\gamma^{-1})\gamma\tau) = f(\gamma\tau)$ by condition (ii). ☐

Let $\gamma \in SL_2(\mathbb{Z})$ be fixed and $q = e^{2\pi i\tau}$. $f(\gamma\tau)$ can be thought of as a function in $q^{\frac{1}{m}}$ which we denote as $F\big(q^{\frac{1}{m}}\big)$, since

$$F\big(q^{\frac{1}{m}}\big) = f(\gamma\tau) = f(\gamma(\tau+m)) = F\big((qe^{2\pi i m})^{\frac{1}{m}}\big) = F\big(q^{\frac{1}{m}}e^{2\pi i}\big) = F\big(q^{\frac{1}{m}}\big)$$

We see that F is defined for $0 < |q^{\frac{1}{m}}| < 1$ as $q^{\frac{1}{m}}$ maps $\mathfrak{h}$ onto the punctured unit disk with centre at origin. Thus $f(\gamma\tau)$ has a Laurent expansion about origin

$$f(\gamma\tau) = \sum_{n=-\infty}^{\infty} a_n (q^{\frac{1}{m}})^n$$

which we say the q-expansion of $f(\gamma\tau)$. Therefore f s a modular function for $\Gamma_0(m)$ iff f satisfies (i) and (ii) of Definition 2.1 and q-expansion of $f(\gamma\tau)$ has finitely many non zero coefficients for negative exponents for all $\gamma \in SL_2(\mathbb{Z})$.

Definition 2.2. (i) A modular function f for $\Gamma_0(m)$ is said to be holomorphic if it is holomorphic on $\mathfrak{h}$.
(ii) A modular function f for $\Gamma_0(m)$ is said to be holomorphic at ∞ if all the negative powers of $q^{\frac{1}{m}}$ in the q-expansion of $f(\gamma\tau)$ has coefficient 0.

Theorem 1.13(ii) and Theorem 1.18 implies that $j(\tau)$ is a modular function for $\Gamma_0(1) = SL_2(\mathbb{Z})$. In the following part we show that a modular function for $SL_2(\mathbb{Z})$ is a rational function in $j(\tau)$.

2.1 Classification of modular functions for $SL_2(\mathbb{Z})$

Lemma 2.1. *A holomorphic modular function for $SL_2(\mathbb{Z})$ which is holomorphic at ∞ is constant.*

Proof. We start by showing that image of $\mathfrak{h} \cup \{i\infty\}$ under f is compact. Let $\{f(\tau_n)\}$ be a sequence in the image. Since f is $SL_2(\mathbb{Z})$ invariant we can assume that $\tau_n \in \{\tau \in \mathfrak{h} \mid |\mathrm{Re}(\tau)| \leq \frac{1}{2}, \mathrm{Im}(\tau) \geq \frac{1}{2}\}$. If $\{\mathrm{Im}(\tau_n) \mid n \in \mathbb{N}\}$ is bounded then τ_n's lie in a compact subset of $\mathfrak{h}$. Hence there is $\tau \in \mathfrak{h}$ such that τ_n converge to τ which then by continuity implies $f(\tau_n)$ converges to $f(\tau)$. If $\{\mathrm{Im}(\tau_n) \mid n \in \mathbb{N}\}$ is unbounded then there is a subsequence τ_{n_k} of τ_n converging to $i\infty$. Now as $\lim_{\tau \to i\infty} f(\tau) = f(\infty)$ exists as a complex number, we have

$$\lim_{k \to \infty} f(\tau_{n_k}) = f\left(\lim_{k \to \infty} \tau_{n_k}\right) = f(\infty)$$

This shows $f(\mathfrak{h} \cup \{i\infty\})$ is compact, so there exists $\tau_0 \in \mathfrak{h} \cup \{i\infty\}$ such that $|f(\tau_0)| \geq |f(\tau)|$ for τ in a neighbourhood of τ_0. From maximum modulus principle it follows that f is constant which is equal to $f(\infty)$. □

Lemma 2.2. *A holomorphic modular function for $SL_2(\mathbb{Z})$ is a polynomial in $j(\tau)$.*

Proof. Withoutloss of generality let f be a holomorphic modular function for $SL_2(\mathbb{Z})$ which is not holomorphic at ∞. The q-expansion of $f(\gamma\tau) = f(\tau)$ has only finite negative powers of q. Let the least negative power $f(\tau)$ has $-n$ for $n \in \mathbb{N}$. We claim that there exists a polynomial $A(x) \in \mathbb{C}[x]$ such that $f(\tau) - A(j(\tau))$ is holomorphic at ∞. We show this by induction on n. If $n = 1$, then q-expansion of $f(\tau)$ is given by $\sum_{k=-1}^{\infty} a_k q^k$ with $a_{-1} \neq 0$. Since q-expansion of $j(\tau)$ starts with $\frac{1}{q}$, the polynomial $A(x) = a_{-1}x$ does the job. By induction assume that our claim is true for n. Let $f(\tau)$ has the least negative power $-(n+1)$. The q-expansion of $f(\tau)$ is given by $\sum_{k=-(n+1)}^{\infty} a_k q^k$ with $a_{-(n+1)} \neq 0$. Then $f(\tau) - a_{-(n+1)}(j(\tau))^{n+1}$ has the least negative power $-n$ which by induction hypothesis implies that $f(\tau) - a_{-(n+1)}(j(\tau))^{n+1} - A(j(\tau))$ is holomorphic at ∞ for some $A(x) \in \mathbb{C}[x]$. Hence $f(\tau) - B(j(\tau))$ holomorphic at ∞ where $B(x) \in \mathbb{C}[x]$ with degree $n+1$. By previous lemma it follows that $f(\tau) - B(j(\tau))$ is constant and therefore $f(\tau)$ is a polynomial in $j(\tau)$. □

Theorem 2.3. *A modular function for $SL_2(\mathbb{Z})$ is a rational function in $j(\tau)$.*

Proof. Let f be a modular function for $SL_2(\mathbb{Z})$. Since f is $SL_2(\mathbb{Z})$ invariant every pole of f is equivalent to one in

$$R = \{\tau \in \mathfrak{h} \mid |Re(\tau)| \leq \frac{1}{2} , Im(\tau) \geq \frac{1}{2}\}$$

Note that f has finite number of poles in R. To see this we use the fact that $f(\tau)$ has a meromorphic q-expansion which implies $f(\tau)$ does not have a pole for $0 < |q| < \epsilon$ where $0 < \epsilon < 1$ as set of poles is isolated. So $f(\tau)$ does not have a pole for $\mathrm{Im}(\tau) > \frac{\log(\frac{1}{\epsilon})}{2\pi}$ which implies poles of f lie in

$$\{\tau \in \mathfrak{h} \mid |Re(\tau)| \leq \frac{1}{2}\ ,\ \frac{1}{2} < Im(\tau) \leq \frac{\log(\frac{1}{\epsilon})}{2\pi}\}$$

which being compact can have finitely many poles.
If $f(\tau)$ has a pole of order m at $\tau_0 \in R$. The function $j(\tau) - j(\tau_0)$ is holomorphic at τ_0 and has a zero at τ_0. Hence $j(\tau) - j(\tau_0) = (\tau - \tau_0)g(\tau)$ for some τ in a neighbourhood of τ_0 and g being holomorphic on the same neighbourhood. This helps us to conclude that $(j(\tau) - j(\tau_0))^m f(\tau)$ is holomorphic at τ_0. Hence $f(\tau)$ is a rational function in neighbourhood of τ_0.
Now let $\tau_1, \tau_2, ..., \tau_n$ be the poles inside R with order $m_1, m_2, ..., m_n$ respectively for some $n \in \mathbb{N}$. Then the function $\prod_{k=1}^{n}(j(\tau) - j(\tau_k))^{m_k} f(\tau)$ is holomorphic on R and by invarinace under $SL_2(\mathbb{Z})$ is holomorphic on $\mathfrak{h}$. By previous lemma $\prod_{k=1}^{n}(j(\tau) - j(\tau_k))^{m_k} f(\tau)$ is a polynomial in $j(\tau)$. Hence $f(\tau)$ is a rational function of $j(\tau)$. □

2.2 Cosets of $C(m)$ in $\Gamma_0(m)$

Theorem 2.4. *Let* $m \in \mathbb{N}$,

$$C(m) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in \mathbb{Z},\ \ ad = m,\ \ a > 0,\ \ 0 \leq b < d,\ \ \gcd(a, b, d) = 1 \right\},$$

$\sigma_0 = \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix}$ *and* $\sigma \in C(m)$. *The set* $\{(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z}) \mid \sigma \in C(m)\}$ *exhaust right coset of* $\Gamma_0(m)$ *in* $SL_2(\mathbb{Z})$.

Proof. **Step-1**
Firstly we claim that $\Gamma_0(m) = (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$. To see this we let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(m)$ so that $c = c_1 m$ for some $c_1 \in \mathbb{Z}$ and let $\eta = \begin{bmatrix} a & bm \\ c_1 & d \end{bmatrix}$ which lies in $SL_2(\mathbb{Z})$ as $ad - bc_1 m = ad - bc = 1 = \det(\gamma)$.

$$\begin{aligned} \sigma_0^{-1}\eta\sigma_0 &= \begin{bmatrix} \frac{1}{m} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & bm \\ c_1 & d \end{bmatrix} \begin{bmatrix} m & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{m} & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} am & bm \\ c_1 m & d \end{bmatrix} = \begin{bmatrix} a & b \\ c_1 m & d \end{bmatrix} = \gamma \end{aligned}$$

Now let $\eta = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in (\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_0) \cap SL_2(\mathbb{Z})$. So $\eta = \sigma_0^{-1}\gamma\sigma_0$ for some $\gamma = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} \in SL_2(\mathbb{Z})$ which implies $c = c_1 m$ and $\eta \in \Gamma_0(m)$.

Step-2
In order to show that the set $\{(\sigma_0^{-1} SL_2(\mathbb{Z})\sigma) \cap SL_2(\mathbb{Z}) \mid \sigma \in C(m)\}$ is a

right coset of $\Gamma_0(m)$ in $SL_2(\mathbb{Z})$ we need to consider the following. Given $\tilde{S} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ we wish to find $\tilde{T} \in SL_2(\mathbb{Z})$ and $\sigma = \begin{bmatrix} a” & b” \\ 0 & d” \end{bmatrix}$ such that $\sigma_0 \tilde{S} = \tilde{T}\sigma$. Let $\tilde{T}^{-1} = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$ and $\sigma_0 \tilde{S} = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$, then $\tilde{T}^{-1}\sigma_0 S = \sigma$ implies $ya' + zc' = 0$. So y, z can be found as a', c' are known. Since $\tilde{T}^{-1} \in SL_2(\mathbb{Z})$, $\gcd(y, z) = 1$ which implies that there exists w, x such that $wz - xy = 1$. $\tilde{T}$ is now determined. So is σ. Now we multiply some special matrices from $SL_2(\mathbb{Z})$ with σ which does not change the coset of σ in $SL_2(\mathbb{Z})$ (say H) and give us another coset representative. Multiplying $T = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$, we have $T\sigma = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a'' & b'' \\ 0 & d'' \end{bmatrix} = \begin{bmatrix} a'' & b'' + kd'' \\ 0 & d'' \end{bmatrix}$ which shows that a coset representative $\sigma_T = \begin{bmatrix} a'' & b''_T \\ 0 & d'' \end{bmatrix}$ for H is possible such that $b_T \in \{0, 1, ..., d'' - 1\}$. Further multiplying $S = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ with σ, we have $S\sigma = \begin{bmatrix} -a'' & b'' \\ 0 & -d'' \end{bmatrix}$ which shows a coset representative $\sigma_S = \begin{bmatrix} a''_S & b'' \\ 0 & d''_S \end{bmatrix}$ for H is possible with $a''_S, b''_S > 0$. Note that $S, T, \tilde{T}, \tilde{S} \in SL_2(\mathbb{Z})$ implies that each of them have entries relatively prime. Furthermore the multiplication of two matrices in $GL_2(\mathbb{Z})$ whose entries are relatively prime has its entries relatively prime. Since the matrices involved in determining σ_S or σ_T, i.e. $\sigma_0\tilde{S}, \tilde{T}^{-1}, S, T$, have entries relatively prime, the entries of σ are also relatively prime.

Step-3

To see that different $\sigma \in C(m)$ give different right cosets, let $\sigma_0^{-1} SL_2(\mathbb{Z})\sigma_1 = \sigma_0^{-1} SL_2(\mathbb{Z})\sigma_2$ for some $\sigma_1, \sigma_2 \in C(m)$. Then for some T_1 and T_2, $\sigma_0^{-1} T_1 \sigma_1 = \sigma_0^{-1} T_2 \sigma_2$ which implies $\sigma_1 = T_1^{-1} T_2 \sigma_2 = T_3 \sigma_2$ for some $T_3 = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in SL_2(\mathbb{Z})$. Now $\sigma_1 = T_3\sigma_2$ implies $\gamma = 0$. Also comparing the entry in the first row and column we have $\alpha > 0$. Then $\alpha\delta = 1$ implies $\alpha = \delta = 1$. Finally comparing the entry in the first row and second column we have $\beta = 0$. Thus $T_3 = I$ and $\sigma_1 = \sigma_2$. $\square$

Let $m \in \mathbb{N}$. As $j(\tau)$ is modular function for $SL_2(\mathbb{Z})$ it is certainly a modular function for $\Gamma_0(m)$. Now we will see that $j(m\tau)$ is a modular function for $\Gamma_0(m)$. $j(m\tau)$ is holomorphic on $\mathfrak{h}$ as $j(\tau)$ is holomorphic on $\mathfrak{h}$. To check the invariance let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(m)$. Then we have

$$j(m\gamma\tau) = j\left(\frac{m(a\tau + b)}{c\tau + d}\right) = j\left(\frac{a(m\tau) + bm}{\frac{c}{m}(m\tau) + d}\right) = j(\gamma' m\tau)$$

where $\gamma' = \begin{bmatrix} a & bm \\ \frac{c}{m} & d \end{bmatrix}$ since $\gamma \in \Gamma_0(m)$ we have $\gamma' \in SL_2(\mathbb{Z})$ which implies

$$j(m(\gamma\tau)) = j(\gamma' m\tau) = j(m\tau)$$

We have shown theorem 2.4 which will help us to compute q-expansion of $j(m\tau)$. Let $\gamma \in SL_2(\mathbb{Z})$ be fixed. By theorem 0.1 choose $\sigma \in C(m)$ such that $\gamma = \sigma_0^{-1}\gamma_1\sigma$ for some $\gamma_1 \in SL_2(\mathbb{Z})$. Now

$$j(m\gamma\tau) = j(\sigma_0\gamma\tau) = j(\gamma_1(\sigma\tau)) = j(\sigma\tau)$$

as $j(\tau)$ is $SL_2(\mathbb{Z})$ invariant. Let $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, then

$$q(\sigma\tau) = e^{\frac{2\pi i(a\tau+b)}{d}} = e^{\frac{2\pi i b}{d}} q^{\frac{a}{d}}$$

If we write $\zeta_m = e^{\frac{2\pi i}{m}}$, then $q(\sigma\tau) = (\zeta_m)^{ab}(q^{\frac{1}{m}})^{a^2}$ as $ad = m$. Thus

$$j(m\gamma\tau) = j(\sigma\tau) = \frac{(\zeta_m)^{-ab}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n\zeta_m)^{abn}(q^{\frac{1}{m}})^{a^2 n}, \;\; c_n \in \mathbb{Z}$$

where

$$j(\tau) = \frac{1}{q} + \sum_{n=0}^{\infty} c(n)q^n$$

There are only finitely many negative powers which shows $j(m\tau)$ is a modular function for $\Gamma_0(m)$.

3 The Modular Equation

In this section we introduce modular equation which will help us to classify modular functions for $\Gamma_0(m)$ and show that $j(\tau)$ is an algebraic integer for τ inside ring of integers of $\mathbb{Q}(\sqrt{-n})$. We begin with a lemma.

Lemma 3.1. *Let $\Gamma_0(m)\gamma_i$ be a right cosets in $SL_2(\mathbb{Z})$ where $i \in \{1, 2, ..., |C(m)|\}$. If*

$$\Phi_m(X,\tau) = \prod_{i=1}^{|C(m)|} \big(X - j(m\gamma_i\tau)\big)$$

then $\Phi_m(X,\tau)$ is a polynomial in X and $j(\tau)$.

Proof. Let us consider the coefficients of powers of X in $\Phi_m(X,\tau)$. The coefficients are symmetric polynomials in $j(m\gamma_i\tau)$'s which are holomorphic on $\mathfrak{h}$. Let $\gamma \in SL_2(\mathbb{Z})$. Then the cosets $\Gamma_0(m)\gamma_i\gamma$'s are a permutation of the cosets $\Gamma_0(m)\gamma_i$'s. Since $j(m\tau)$ is invariant under $\Gamma_0(m)$, $j(m\gamma_i\gamma\tau)$'s are a permutation of $j(m\gamma_i\tau)$. The coefficients being symmetric polynomials remains same under the action of permutations. Hence the coefficients are invariant under $SL_2(\mathbb{Z})$.

For each i, we have $j(m\gamma_i\tau) = j(\sigma\tau)$ for $\sigma \in C(m)$. However from the proof of previous theorem the q-expansion of $j(\sigma\tau)$ has finitely many negative exponents. The coefficients are then polynomials in $j(\sigma\tau)$'s which implies that the coefficients will again have finitely many negative exponents. This shows coefficients of powers of X in $\Phi_m(X,\tau)$ are holomorphic modular functions, hence are polynomials in $j(\tau)$. Therefore there is a polynomial $\Phi_m(X,Y) \in \mathbb{C}[X,Y]$ such that

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} \big(X - j(m\gamma_i\tau)\big)$$

$\square$

The equation $\Phi_m(X,Y) = 0$ is called **the modular equation** and by abuse of terminology we will call $\Phi_m(X,Y)$ as the modular equation. Each $j(m\gamma_i\tau)$ can be written as $j(\sigma\tau)$ for a unique $\tau \in C(m)$ which lets us to write the modular equation in the form

$$\Phi_m(X, j(\tau)) = \prod_{i=1}^{|C(m)|} \big(X - j(\sigma\tau)\big)$$

Lemma 3.2. *Let $m \in \mathbb{N}$. Then $\Phi_m(X,Y)$ is irreducible as a polynomial in X.*

Proof. Let γ_i be right coset representative for $\Gamma_0(m)$ in $SL_2(\mathbb{Z})$. Let F_m be the field $\mathbb{C}(j(\tau), j(m\tau))$. Since $\Phi_m(X, j(\tau))$ has coefficients in $\mathbb{C}(j(\tau))$ and $j(m\tau)$ is a root, it follows that $[F_m : \mathbb{C}(j(\tau))] \leq |C(m)|$. Our goal will be to prove the equality which would then imply the minimal polynomial of $j(m\tau)$ over $\mathbb{C}(j(\tau))$ and irreducibility will follow. Let F be the field of all meromorphic functions on $\mathfrak{h}$ which contains F_m as a subfield. Now let $\phi_\gamma : F_m \to F$ defined as $\phi(f(\tau)) = f(\gamma\tau)$ for $\gamma \in SL_2(\mathbb{Z})$. We claim that ϕ_γ is injective and is identity on $\mathbb{C}(j(\tau))$. Note that $\phi_\gamma(j(\tau)) = f(j(\gamma\tau)) = f(j(\tau))$ which implies ϕ_γ is identity on $\mathbb{C}(j(\tau))$. If $\phi_\gamma(f_1) = \phi_\gamma(f_2)$, then $f_1(\gamma\tau) = f_2(\gamma\tau)$ for $\tau \in \mathfrak{h}$. Both f_1 and f_2 are meromorphic on $\mathfrak{h}$ and $\gamma\tau = \frac{a\tau+b}{c\tau+d}$ for $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, is an open set as τ varies over $\mathfrak{h}$ by open mapping theorem. Since f_1 and f_2 agree on a open set, they agree on $\mathfrak{h}$. Thus ϕ_γ is injective.

Note that $j(m\gamma_i\tau) \neq j(m\gamma_j\tau)$ for $i \neq j$. To see this we first note that $j(m\gamma_i\tau) = j(\sigma_i\tau)$ and $j(m\gamma_j\tau) = j(\sigma_j\tau)$ for $\begin{bmatrix} a_i & b_i \\ 0 & d_i \end{bmatrix} = \sigma_i \neq \sigma_j = \begin{bmatrix} a_j & b_j \\ 0 & d_j \end{bmatrix}$ both inside $C(m)$. If possible suppose $j(\sigma_i) = j(\sigma_j)$, then the least power q-expansion of both is a_i^2, a_j^2 which are equal and imply $a_i = a_j$ as $a_i, a_j > 0$. $\sigma_i, \sigma_j \in C(m)$ then implies $d_i = d_j$. Furthermore on considering coefficients of $(q^{\frac{1}{m}})^{a_i^2}$, we have $\zeta_m^{a_i(b_i-b_j)} = 1$, however $(b_i - b_j) \in \{0, 1, ..d-2\}$ implies $b_i = b_j$, consequently $\sigma_i = \sigma_j$ which is a contradiction.

Now for each $\gamma_i \in C(m)$ we may consider ϕ_{γ_i} which are distinct as $j(m\gamma_i) \neq j(m\gamma_j)$ and belongs to the field extension $F_m/\mathbb{C}(j(\tau))$. This shows $[F_m : \mathbb{C}(j(\tau))] \geq |C(m)|$ and our desired equality is proved. $\square$

3.1 Classification of modular functions for $\Gamma_0(m)$

Now we will us the above lemmas to classify modular function for $\Gamma_0(m)$.

Theorem 3.3. *A modular function for $\Gamma_0(m)$ is a rational function of $j(\tau)$ and $j(m\tau)$.*

Proof. Let f be a modular function for $\Gamma_0(m)$. We consider the function

$$G(X,\tau) = \Phi_m(X, j(\tau)) \sum_{i=1}^{|C(m)|} \frac{f(\gamma_i\tau)}{X - j(m\gamma_i\tau)}$$

$$= \sum_{i=1}^{|C(m)|} f(\gamma_i\tau) \prod_{j\neq i} \big(X - j(m\gamma_i\tau)\big)$$

$G(X,\tau)$ is a polynomial in X. We claim that coefficients of X in $G(X,\tau)$ are modular function for $SL_2(\mathbb{Z})$. The proof is similar to proof in Lemma 3.1 where we use the fact that coefficients of X are symmetric polynomials in $f(\gamma_i\tau)$'s, $j(m\gamma_i\tau)$'s and $f(\gamma_i\tau)$ has q-expansion with finite negative exponents. Since a modular function for $SL_2(\mathbb{Z})$ is a polynomial in $j(\tau)$, $G(X,\tau)$ is a polynomial $G(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$. Without loss of generality we assume γ_1 is the identity matrix. Note that in $\Phi_m(X, j(\tau))$ one of the σ is γ_1 which implies

$$\Phi_m(j(m\tau), j(\tau)) = \big((j(m\tau) - j(m\gamma_1\tau)\big) \prod_{i=2}^{|C(m)|} \big(j(m\tau) - j(m\gamma_i\tau)\big) = 0$$

Now using this and product rule of differentiation we have

$$\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau)) = \prod_{j\neq i} \big(j(m\tau) - j(m\gamma_j\tau)\big)$$

On putting $X = j(m\tau)$ in $G(X, j(\tau))$ we have

$$G(j(m\tau), j(\tau)) = f(\tau)\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau))$$

$\Phi_m(X, j(\tau))$ is irreducible, so it can not have repeated roots which implies $\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau)) \neq 0$.
Therefore we can write

$$f(\tau) = \frac{G(j(m\tau), j(\tau))}{\frac{\partial\Phi_m}{\partial X}(j(m\tau), j(\tau))}$$

which is a rational function in $j(\tau)$ and $j(m\tau)$. □

3.2 Arithmetic properties of $\Phi_m(X,Y)$

Now we will explore some arithmetic properties of the Modular Equation.

Theorem 3.4. *Let $m \in \mathbb{N}$, then $\Phi_m(X,Y) \in \mathbb{Z}[X,Y]$.*

Proof. Let $f(\tau)$ be an elementary symmetric function in $j(\sigma\tau)$'s for $\sigma \in C(m)$. Let us denote $\zeta_m = e^{\frac{2\pi i}{m}}$. Now $f(\tau) \in \mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$ where $\mathbb{Q}(\zeta_m)((q^{\frac{1}{m}}))$ denotes the field of formal meromorphic Laurent series. We claim that $f(\tau) \in \mathbb{Q}((q^{\frac{1}{m}}))$. An automorphism $\psi \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is determined by how it acts on the coefficient of exponents of $q^{\frac{1}{m}}$.
If $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(m)$, then $\psi(\zeta_m) = \zeta^k$ where $0 < k < m$ is relatively prime to m. To see this we note that ψ sends ζ_m to some other root of $x^m - 1 = 0$. Suppose that $\gcd(k,m) > 1$, then

$$\psi\left(\zeta_m^{\frac{lcm(k,m)}{k}}\right) = \left(\zeta_m^k\right)^{\frac{lcm(k,m)}{k}} = \left(\zeta_m^m\right)^{\frac{lcm(k,m)}{m}} = 1 = \psi(1)$$

which is a contradiction as

$$0 < \frac{lcm(k,m)}{k} = \frac{m}{\gcd(k,m)} < m$$

which implies $\zeta_m^{\frac{lcm(k,m)}{k}} \neq 1$ subsequently ψ is not injective.
From the expansion of $j(\sigma\tau)$ we have

$$\psi(j(\sigma\tau)) = \frac{\zeta_m^{-abk}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{abkn} (q^{\frac{1}{m}})^{a^2 n}$$

as all of the c_n's are integers. Now $\gcd(bk,m) = 1$ implies that $\gcd(bk,d) = 1$, hence there exists $b' \in \{0,1,...,d-1\}$ such that $b' \equiv bk \pmod{d}$. So we have

$$\zeta_m^{abk} = \zeta_m^{a(b'+td)} = \zeta_m^{ab'} \left(\zeta_m^m\right)^t = \zeta_m^{ab'}$$

where $b' = bk - td$ for some integer t and $ad = m$. The above formula can be written as

$$\psi(j(\sigma\tau)) = \frac{\zeta_m^{-ab'}}{(q^{\frac{1}{m}})^{a^2}} + \sum_{n=0}^{\infty} c_n \zeta_m^{ab'n} (q^{\frac{1}{m}})^{a^2 n}$$

If we let $\sigma' = \begin{bmatrix} a & b' \\ 0 & d \end{bmatrix} \in C(m)$, then $\sigma' \in C(m)$ and by q-expansion of $j(\sigma'\tau)$ we will have $\psi(j(\sigma\tau)) = j(\sigma'\tau)$. Thus an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ permutes $j(\sigma\tau)$'s. Since $f(\tau)$ is symmetric in $j(\sigma\tau)$'s it follows that $f(\tau) \in \mathbb{Q}((q^{\frac{1}{m}}))$.
While proving Lemma 3.1, we saw that $f(\tau)$ is a polynomial in $j(\tau)$ which implies $f(\tau) \in \mathbb{Q}((q))$. Since the coefficients of q-expansion of $f(\tau)$ are algebraic integers and also belong to $\mathbb{Q}$, it follows that $f(\tau) \in \mathbb{Z}((q))$. Hence we have $A(X) = a_n X^n + ... + a_0 \in \mathbb{C}[X]$ for some $n \in \mathbb{N}$ such that $f(\tau) = A(j(\tau))$.

We are required to show that $A(X)$ is an integer polynomial. Note that the coefficient of q^{-n} in q-expansion of $A(j(\tau))$ is a_n which is integer as the q-expansion of $f(\tau)$ has integer coefficients. To show $a_{n-1} \in \mathbb{Z}$ we consider the coefficient of $q^{-(n-1)}$ in q-expansion of $f(\tau) - a_n j((\tau))^n$ which is a integer and equals to a_{n-1} as $f(\tau) - a_n j((\tau))^n = a_{n-1}(j(\tau))^{n-1} + ... + a_0$. Since n is finite, we can similarly show that $a_t \in \mathbb{Z}$ for $t \in \{n-2, ..., 0\}$. ☐

Theorem 3.5. *Let m is a natural number and m is not a perfect square, then $\Phi_m(X, X)$ is a polynomial of degree > 1 whose leading coefficient is ± 1.*

Proof. Let m be a non square natural number. Let

$$\Phi(X, Y) = a_{n_1,n_2} X^{n_1} Y^{n_2} + ... + a_0$$

be such that a_{n_1,n_2} is the leading coefficient of $\Phi(X, Y)$ for some $n_1, n_2 \in \mathbb{N}$. Then $\Phi(X, X) = a_{n_1,n_2} X^{n_1+n_2} + ... + a_0$. Our aim is to show $a_{n_1,n_2} = \pm 1$. If we replace X with $j(\tau)$, then the leading coefficient is the coefficient of most negative power of q in the q-expansion of $\Phi_m(j(\tau), j(\tau))$. Firstly we consider the q-expansion of one of the factor $j(\tau) - j(\sigma\tau)$ for $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(m)$ which is given by

$$j(\tau) - j(\sigma\tau) = \frac{1}{q} - \frac{\zeta_m^{-ab}}{q^{\frac{a}{d}}} + \sum_{n=0}^{\infty} d_n \left(q^{\frac{1}{m}}\right)^n$$

for some coefficient $d_n \in \mathbb{C}$. Since $ad = m$, $a \neq d$ which implies the coefficient of most negative power of q in q-expansion of $j(\tau) - j(\sigma\tau)$ is either ζ_m^{-ab} or 1. So in any case the coefficient is a root of unity. Since $\Phi(j(\tau), j(\tau))$ is product of $j(\tau) - j(\sigma\tau)$'s as σ varies over $C(m)$, a_{n_1,n_2} is a root of unity which is also an integer by the previous theorem. Thus a_{n_1,n_2} is either $+1$ or -1. ☐

3.3 Correspondence between roots of $\Phi_m(X, Y)$ and cyclic sublattices of index m

Definition 3.1. Let L be a lattice and L' be a sublattice inside L. L' is said to be cyclic sublattice of L if the group L'/L is cyclic. Furthermore L' is said to be of index m if $|L'/L| = m$

Lemma 3.6. *Let $M = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, A be an integer matrix with* $\det(A) \neq 0$. *Then the group M/AM is cyclic if and only if the entries of A are relatively prime.*

Proof. **Step-1**
We begin by proving the claim which states that a finite abelian group G is not cyclic if and only if there exists a subgroup of it isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$ for some $n \in \mathbb{N}$ and $d > 1$. Let G is not cyclic and $|G| = n = p_1^{t_1}...p_r^{t_r}$ be prime factorisation of m, then by fundamental theorem of abelian groups we have $G \cong \mathbb{Z}_{q_1^{s_1}} \oplus ... \mathbb{Z}_{q_l^{s_l}}$ where $q_1, .., q_l$ are one of p_i's and $s_i \geq 1$ for all i. We claim that

there exists $q_{i_0} \neq q_{j_0}$ for some i_0, j_0 such that $\gcd(q_{i_0}, q_{j_0}) = d \neq 1$. Suppose not then $\gcd(q_i, q_j) = 1$ for $i \neq j$ for all i, j, so $\gcd(q_i^{s_i}, q_j^{s_j}) = 1$ which implies $\mathbb{Z}_{q_i^{s_i}} \oplus \mathbb{Z}_{q_j^{s_j}} \cong \mathbb{Z}_{q_i^{s_i} q_j^{s_j}}$. Similarly arguing for other q_k's we have $\mathbb{Z}_{q_1^{s_1}} \oplus ... \mathbb{Z}_{q_l^{s_l}} \cong \mathbb{Z}_m$ which is a contradiction since G is cyclic. Since d divides both q_{i_0} and q_{j_0}, both $\mathbb{Z}_{q_{i_0}}$ and $\mathbb{Z}_{q_{j_0}}$ have a subgroup isomorphic to $\mathbb{Z}_d$. Without loss of generality we can assume $i_0 = 1$ and $j_0 = 1$. Now we let $H = \mathbb{Z}_d \oplus \mathbb{Z}_d \oplus \mathbb{Z}_1 \oplus ... \oplus \mathbb{Z}_1$. Clearly H is a subgroup of G isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$. Furthermore if G has a subgroup isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$, then G is not cyclic as subgroup of every cyclic is cyclic and $(\mathbb{Z}/d\mathbb{Z})^2$ is not cyclic.

Step-2

In Step-2 we use Step-1 to show if A has a common divisor $d > 1$, then M/AM is not cyclic. A can be written as dA' for some integer matrix A. Now consider $A'M/dA'M = A'M/AM \subset M/AM$ is a subgroup of M/AM. $A'M$ is a lattice with dimension 2, hence $A'M/dA'M$ as a group is isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$. Thus by Step-1, M/AM is not cyclic.

Step-3

Assume that M/AM is not cyclic. By Step-1, there exists $AM \subset M' \subset M$ such that $M'/AM \cong (\mathbb{Z}/d\mathbb{Z})^2$. Let $g \in M'$, then $d(g + AM) = AM = dg + AM$ as every non zero element of M'/AM has order d. Hence $dM' \subset AM$. We have the inclusions $dM' \subset AM \subset M'$ such that both M'/AM and M'/dM' isomorphic to $(\mathbb{Z}/d\mathbb{Z})^2$ which implies $AM = dM'$. We claim that d divides entries of A. Let $M = \mathbb{Z}e'_1 \oplus \mathbb{Z}e'_2$, $A = \begin{bmatrix} a & b \\ c & d' \end{bmatrix}$ and $e'_1 = \alpha e_1 + \beta e_2$, $e'_2 = \gamma e_1 + \delta e_2$. Now $AM = dM'$ implies

$$\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}(ce_1 + d'e_2) = \mathbb{Z}((d\alpha)e_1 + (d\beta)e_2) \oplus \mathbb{Z}((d\gamma)e_1 + (d\delta)e_2)$$

Therefore $a = d\alpha$, $b = d\beta$, $c = d\gamma$ and $d' = d\delta$ and we are done. □

Lemma 3.7. *Let $\tau \in \mathfrak{h}$, L' be a sublattice of $L = \mathbb{Z} \oplus \mathbb{Z}\tau$ of finite index and d be the smallest positive integer in L'. Then $L' = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + b)$ for some $a, b \in \mathbb{Z}$.*

Proof. Let $L' = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$ where $e_1, e_2 \in L$. Since $e_1, e_2 \in L$, we can let $e_1 = d' + c\tau$ and $e_2 = a + b\tau$ where $a, b, c, d' \in \mathbb{Z}$. Now let $d = k_1(d' + c\tau) + k_2(a + b\tau)$ for some $k_1, k_2 \in \mathbb{Z}$. This implies $k_1 d' + k_2 a = d$ and as d is the smallest positive integer inside L' it follows that $\gcd(a, d') = d$ which in turn implies $a = \alpha d$ and $d' = \beta d$ for some $\alpha, \beta \in \mathbb{Z}$. Thus $L' = \mathbb{Z}(d + c\tau) \oplus \mathbb{Z}(d + b\tau)$.One can then choose another basis of L' such that $c = 0$. □

Lemma 3.8. *Let $\tau \in \mathfrak{h}$, $\sigma, \sigma' \in C(m)$. If $\mathbb{Z}d \oplus \mathbb{Z}(d\sigma\tau) = \mathbb{Z}d' \oplus \mathbb{Z}(d'\sigma'\tau)$, then $\sigma = \sigma'$.*

Proof. Let $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$ and $\sigma' = \begin{bmatrix} a' & b' \\ 0 & d' \end{bmatrix}$. The smallest positive integer in $\mathbb{Z}d \oplus \mathbb{Z}(d\sigma\tau)$ is d. Suppose not, then let $t \in \{1, 2, ..d - 1\}$ such that $t = k_1 d + k_2(a\tau + b)$ which implies $dk_1 + bk_2 = t$ and $k_2 a = 0$. Hence $k_2 = 0$ and t is a multiple of d which is a contradiction. Similarly d' is the smallest positive integer in $\mathbb{Z}d' \oplus \mathbb{Z}(d'\sigma'\tau)$. Thus $d = d'$. Again $\sigma, \sigma' \in C(m)$ implies that $a = a'$. Let $a\tau + b = k_1'd + k_2'(a\tau + b')$. This implies $k_2' = 1$ and $b - b' = k_1'd$. Since $b, b' \in \{0, 1, .., d-1\}$, $k_1' = 0$ and the proof is complete. ☐

Lemma 3.9. *Let* $\tau \in \mathfrak{h}$ *and* $L = \mathbb{Z} \oplus \mathbb{Z}\tau$. *Then*
(i) Givn a cyclic sublattice $L' \subset L$ *of index* m *there is a unique* $\sigma \in C(m)$ *such that* $L' = \mathbb{Z}d \oplus \mathbb{Z}(d\sigma\tau)$
(ii) Conversely if $\sigma = \begin{bmatrix} a & b \\ 0 & d' \end{bmatrix} \in C(m)$, *then* $\mathbb{Z}d \oplus \mathbb{Z}(d\sigma\tau)$ *is a cyclic sublattice of* L *with index* m.

Proof. Let $L' \subset L$ is cyclic of index m. If d is the smallest positiv integer in L', then by lemma $L' = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + b)$ for some integer a, b. We may assume that $a > 0$ and since index of L' is given by $\det(\sigma)$ where $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, we have $ad = m$. If k is an integer then $\mathbb{Z}d \oplus \mathbb{Z}((a\tau + b) + kd) = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + (b + kd))$. Thus we can choose k in such a way that $0 \leq b < d$. As L' is cyclic by lemma $\gcd(a, b, d) = 1$. Hence $\sigma = \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in C(m)$. Furthermore $L' = \mathbb{Z}d \oplus \mathbb{Z}(a\tau + b) = d(\mathbb{Z} \oplus \mathbb{Z}\frac{(a\tau+b)}{d}) = d(\mathbb{Z} \oplus \mathbb{Z}\sigma\tau)$.
Proof of (ii) follows from lemma 3.6 since $\gcd(a, b, d') = 1$ implies $\mathbb{Z}d \oplus \mathbb{Z}(d\sigma\tau)$ is cyclic sublattice and $\det(\sigma) = m$ implies it is of index m. ☐

Theorem 3.10. *Let* m *be a positive integer. Let* $u, v \in \mathbb{C}$. *Then* $\Phi_m(u, v) = 0$ *if and only if there exists a lattice* L *and a cyclic sublattice* $L' \subset L$ *of index* m *such that* $u = j(L')$ *an* $v = j(L)$.

Proof. On applying the above lemma j-invariant of a cyclic sublattice L' of index m of $\mathbb{Z} \oplus \mathbb{Z}\tau$ are given by

$$j(L') = j(d(\mathbb{Z} \oplus \mathbb{Z}\sigma\tau)) = j(\mathbb{Z} \oplus \mathbb{Z}\sigma\tau) = j(\sigma\tau)$$

Now by

$$\Phi_m(X, j(\tau)) = \prod_{\sigma' \in C(m)} (X - j(\sigma'\tau))$$

it follows that the roots of $\Phi_m(X, j(\tau)) = 0$ are exactly the j-nvariants of cyclic sublattice of index m of $\mathbb{Z} \oplus \mathbb{Z}\tau$.
Let $u, v \in \mathbb{C}$ such that $j(u, v) = 0$. Since j is surjective there exists $\tau \in \mathfrak{h}$ such that $j(\tau) = v = j(\mathbb{Z} \oplus \mathbb{Z}\tau)$ by definition. Again

$$\Phi_m(X, j(\tau)) = \prod_{\sigma' \in C(m)} (X - j(\sigma'\tau))$$

implies $u - j(\sigma\tau) = 0$ for some $\sigma \in C(m)$. Hence $u = j(\mathbb{Z} \oplus \mathbb{Z}\sigma\tau)$. The proof is done, once we let $L = \mathbb{Z} \oplus \mathbb{Z}\tau$ and $L' = \mathbb{Z} \oplus \mathbb{Z}\sigma\tau$. One may also note the fact that L' is cyclic sublattice with index m follows from lemma 3.6. ☐

3.4 Ring of integers of $\mathbb{Q}(\sqrt{-n})$

Now our main focus will be to consider the ring of integers of imaginary quadratic field extension of $\mathbb{Q}$ which is given by

$$\mathbb{Q}(\sqrt{-n}) = \{p + q\sqrt{-n} \mid p, q \in \mathbb{Q}\}$$

where $n \in \mathbb{N}$ is a square free integer. Note that n is a square free integer iff its prime factorization in $\mathbb{Z}$ does not contain any even powered prime number.

Definition 3.2. Let $a \in \mathbb{Q}(\sqrt{-n})$. Then a is an algebraic number if there exists a polynomial $P(X) \in Z[X]$ such that $P(a) = 0$. Furthermore a is an algebraic integer if there exists $P(X) \in Z[X]$ with leading coefficient 1 such that $P(a) = 0$.

Definition 3.3. The ring of integers of $\mathbb{Q}(\sqrt{-n})$ is defined to be the set of algebraic integers in $\mathbb{Q}(\sqrt{-n})$.

Theorem 3.11. *Let $n \in N$ be a square free integer. The ring of integers of $\mathbb{Q}(\sqrt{-n})$ is given by $\mathbb{Z} \oplus \mathbb{Z}(\sqrt{-n})$ if $n \not\equiv 3 \pmod 4$ and $\mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{-n}}{2})$ if $n \equiv 3$ (mod 4)*

Proof. Let $p + q\sqrt{-n} \in \mathbb{Q}(\sqrt{-n})$. We know that if $p + q\sqrt{-n}$ satisfies a polynomial in $Z[X]$, then $p - q\sqrt{-n}$ also satisfies the polynomial. Hence we consider the polynomial $(X - p - q\sqrt{-n})(X - p + q\sqrt{-n}) = X^2 - 2pX + (p^2 + nq^2)$. To have $p + q\sqrt{-n}$ as an algebraic integer, it is necessary to have $2p, p^2 + nq^2 \in \mathbb{Z}$. We consider two cases, i.e. when $p = k$, $k \in \mathbb{Z}$ and $p = \frac{k}{2}$ for some $k \in \mathbb{Z}$, k is odd.
For the second case, i.e. when $p = \frac{k}{2}$ and k is odd, $p^2 + nq^2 \in \mathbb{Z}$ implies $\frac{k^2}{4} + nq^2 \in \mathbb{Z}$. This forces $q = \frac{k'}{2}$ for some $k' \in \mathbb{Z}$ as n is square free. Since k is odd, $k^2 \equiv 1 \pmod 4$, this implies $nk'^2 \equiv 3 \pmod 4$. However when k' is odd, we have $n \equiv 3 \pmod 4$. Conversely if $n \equiv 3 \pmod 4$, $p + q\sqrt{-n}$ is an algebraic integer where p is an half integer and q is either an integer or half integer. Hence the ring of integer is given by $\mathbb{Z}(\frac{1}{2}) \oplus \mathbb{Z}(\frac{\sqrt{-n}}{2}) = \mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{-n}}{2})$.
For the first case $p = k$ we have $nq^2 \in \mathbb{Z}$. Since n is square free, $q \in \mathbb{Z}$. To see this let $q = \frac{p_1}{q_1}$ for $p_1, q_1 \in \mathbb{Z}$ and $q_1 \neq 0$. $nq^2 \in \mathbb{Z}$ implies q_1^2 divides n which is a contradiction. Conversely if $n \not\equiv 3 \pmod 4$, $p + q\sqrt{-n}$ is an algebraic integer where p and q are integers. Thus the ring of integer is given by $\mathbb{Z} \oplus \mathbb{Z}(\sqrt{-n})$ $\square$

Now we prove the final theorem in the thesis.

Theorem 3.12. *Let O_K be the ring of integers of $K = \mathbb{Q}(\sqrt{-n})$. Then $j(O_K)$ is an algebraic integer.*

Proof. From the previous theorem we have $O_K = \mathbb{Z} \oplus \mathbb{Z}\tau$ where $\tau = \sqrt{-n}$ or $\frac{1+\sqrt{-n}}{2}$. Consider the lattice $O'_K = \sqrt{-n}(O_K) = \mathbb{Z}(\sqrt{-n}) \oplus \mathbb{Z}(\tau\sqrt{-n})$ for $\tau = \sqrt{-n}$. O'_K has basis $\{\sqrt{-n}, -n\}$ where we can write $-n = -n.1 + 0.\sqrt{-n}$ and $\sqrt{-n} = 0.1 + 1.\sqrt{-n}$ which implies $O'_K = AO_K$ where $A = \begin{bmatrix} 0 & 1 \\ -n & 0 \end{bmatrix}$.

Since $\det(A) = n$ and $\gcd(1, -n) = 1$, O'_K is a cyclic sub lattice of O_K by lemma 3.6 with index n. Hence by theorem 3.10

$$0 = \Phi_n(j(\sqrt{-n}O_K), j(O_K)) = \Phi_n(j(O_K), j(O_K))$$

as $j(\sqrt{-n}O_K) = j(O_K)$ by theorem 1.8. NOw $j(O_K)$ is a root of the polynomial $\Phi_n(X, X)$. Since $\Phi_n(X, Y) \in \mathbb{Z}[X, Y]$, $j(O_K)$ is an algebraic number. Again n is square free implies n is not a perfect square. Therefore the leading coefficient of $\Phi_n(X, X)$ is ± 1 and $j(O_K)$ is an algebraic integer as without loss of generality we can take the leading coefficient to be 1. Arguing similarly we can prove for $\tau = \frac{1+\sqrt{-n}}{2}$, $j(O_K)$ is an algebraic integer. $\square$

References

1. *David A. Cox* , **Primes of the form $\mathbf{x}^2+ny^2$**, *John Wiley and Sons, Inc.*, 1989.
2. *Tom M. Apostol* , **Modular Functions and Dirichlet Series in Number Theory**, *Graduate Texts in Mathematics* 41, *Springer*, 1989.